ASSA ABLOY

The following article has been written by Phil Libin with exclusivity for the ASSA ABLOY Future Lab. Mr. Libin is the President of CoreStreet Ltd, a Boston, MA-based technology company that enables convergence of physical and IT security systems.

Is iris scanning better than hand geometry? Are central government databases of everyone's biometric data a prelude to the worst kind of Orwellian dystopia? Who knows? What we do know are a few simpler things about the state biometrics today. Namely, what are today's biometric systems good at? What are they bad at? And why?

A practical summary of the advantages and drawbacks of today's biometric systems for mainstream customers

The field of biometrics is a polarizing and controversial topic, with multiple voices debating the advantages and merits of the technology. Many of the discussions have focused on hypothetical, deeply technical and philosophical issues. Is iris scanning better than hand geometry? Will people ever get over the social stigma of getting their finger prints taken? Are central government databases of everyone's biometric data a prelude to the worst kind of Orwellian dystopia?

We don't know.

What we do know are a few simpler things about the state biometrics today. Namely, what are today's biometric systems good at? What are they bad at? Why? These practical questions haven't been covered with nearly the same volume of ink as the larger issues, but we think that straightforward questions deserve an honest attempt at straightforward answers. That's what this article will try to do in high-level, non-technical terms. Read the conclusions for our quick appraisal of the industry below, or continue reading if you want some more details.

Conclusion

There have been many advances in practical biometric technology over the past few years, but most biometrics-based products do not yet live up to the full potential of the industry. How useful biometrics are to you today will largely depend on what kind of application you have in mind:

Face recognition biometric systems are starting to make a major impact in the surveillance field. If your job is monitoring 10,000 cameras in a large city, you should be looking seriously at what biometrics can do for you today and over the next few years.

Fingerprint scanning has finally become mainstream-useful for access control to computers and electronic files. Fingerprints make logging on to multiple applications relatively easy, and readers are starting to crop up on laptops, cell phones and PDAs. For now, IT-access biometrics aren't really having much of a security impact, so the short-term selling point is cost savings and convenience. If you're in charge of IT for a medium or large-sized enterprise (especially in compliance-intensive industries like government, health care and financial services), you're likely to find something useful here, and early adopters will get real value. However, the mainstream market for IT biometrics probably won't arrive until later in the decade, so if your organization is slow to embrace new technologies, you can safely give biometrics a pass for another year or two. Non-fingerprint systems are showing lots of promise, but there are few practical products that use them for corporate IT control today.

Physical access control applications, however, are another matter. Biometric systems continue to struggle to find a niche at access control; using your fingerprint or iris to open a door is a very natural idea, but the details are still just a bit too cumbersome for mainstream use. High-security areas and other niche environments can benefit from iris scanners, fingerprint readers and hand geometry readers today, but most doors and locks are going to remain biometric-free for the foreseeable future.

Compared to What?

Since a biometric is just another type of authentication factor (in other words, another way to prove who you are), it's worth looking at biometrics in general compared to other ways of accomplishing the same authentication task: passwords, metal keys and electronic access control devices.

Advantages of Biometrics over Passwords

- Passwords are hard to remember, biometrics are always with you.
- You have to change passwords periodically to keep them secure. That's a big hassle for many people (and a big hassle inevitably means poor compliance which means poor security). Biometrics are always with you and never change.
- Passwords can be lost or stolen, and anyone with your password can effectively pretend to be you. Biometrics are very difficult to steal (and even more difficult to lose). While we're on the subject, it's worth pointing out that severed body parts will not fool the majority of modern biometric systems.
- Forgotten passwords generate a large volume of very expensive support desk calls at many large-sized organizations.

Advantages of Passwords over Biometrics

- You don't need to buy any extra products to use passwords.
- As long as you remember them, passwords are very quick and reliable.

Advantages of Biometrics over Physical Keys

- A physical key can typically only get you into a single door – or a number of identically-keyed doors, so you have to carry a large number of keys. A biometric can be used to identify you to any number of access systems.
- A key can be lost or stolen or (sometimes) duplicated.

Disadvantages of Biometrics over Physical Keys

- Metal keys have been around for thousands of years and we've pretty much figured out how to make them exactly right – secure, cheap and reliable.

Advantages of Biometrics over Electronic Keys, Dongles and Access Cards

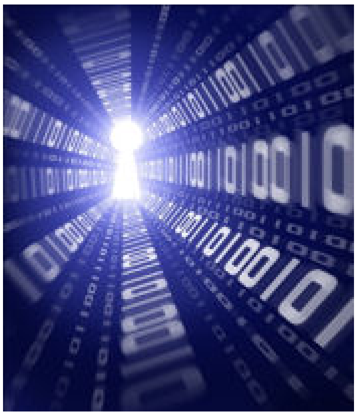
- Biometrics can't be lost or stolen, all the rest can be.
- Biometrics don't require you to carry around anything other than the body parts you normally bring with you anyway.
- Unlike some of the more cumbersome dongles that require you to read an access code off one screen and type it into another one, biometrics are (at least potentially) quick and easy to use.

Disadvantages of Biometrics over Electronic Keys, Dongles and Access Cards

- Physical tokens are usually more reliable than pure biometrics.
- Physical dongles don't suffer from the social stigma associated with some biometrics technologies.

Even though biometrics has some advantages over other types of authentication factors, the best systems combine the two. A finger print template stored on a smart card, for example, is a more reliable combination than just a fingerprint by itself. Read more in the section on biometric accuracy for a partial set of reasons.

Are Biometric Systems Accurate?



The accuracy of most biometrics systems can be tuned by balancing two competing types of errors: false positives and false negatives. Let’s look at the case of fingerprints, although the basic idea is applicable to all other types as well. A false positive error occurs when a bad guy's fingerprint gets mistakenly matched for a good guy's fingerprint. A false negative error occurs when a good guy's fingerprint doesn't get recognized at all. Since fingerprint scanning produces slightly different results each time, the system must be configured with a certain tolerance level. If the tolerance level is very loose, you can virtually eliminate false negatives at the cost of greatly increasing false positives. The system basically says, "Well, it sort of looks like a fingerprint - go on in." If the tolerance level is very strict, you get the opposite effect: "Your fingerprint is off by 0.00001 millimeters - no access for you!"

The accuracy rate is also heavily influenced by how many possible fingerprint matches the system has to consider. If the system has to match your scan against a large database of enrolled fingerprints (called a "one-to-many" match), it's far more likely to come up with a false positive ("hmmm, it kind of looks like user #7654231") and somewhat more likely to come up with a false negative ("it could be this guy or that guy, I better just punt"). Many modern systems avoid this problem by matching your fingerprint against only one possible user - the user stored in your card or other credential - so the chances of a false positive are very low because someone trying to trick the system can't just match anyone's fingerprint; they have to match your fingerprint. Also, the match tolerance can be set very high thereby further reducing the chances of a false positive but increasing the chances of a false negative.

So you can virtually eliminate the false positives (and therefore security risks associated with biometric access), but doesn't the relatively high false negative rate mean that legitimate users will be frequently locked out? Not necessarily; it depends on the penalty for getting a false negative. In most physical access and IT applications, if you get a false negative, you just have to scan your finger a second time so a high false-negative rate is an inconvenience, not a security issue. Let's say it takes you 2 seconds to scan your finger and the false negative error rate is 5%. Most of the time (95%) you'll get access in two seconds. Most of the rest of the time (99.75%) you'll get in with two swipes and four seconds. Every 400 tries or so, you'll have to wait six seconds.

In other words, for applications that don’t heavily penalize users for false negatives, biometric systems can usually be tuned to an acceptably high level of accuracy.

There’s always a catch

Unfortunately, for every type of biometric, there is a small number of people who simply cannot be identified by that method. A small minority of people have fingerprints that are very difficult to enroll. Certain serious diseases of the eye make eye recognition impossible. Some disabled individuals do not have the necessary use of their hands or voice to perform hand geometry or voice pattern matching. These natural limitations mean that biometric systems covering large populations, no matter how accurately tuned, must usually be installed with backup authentication methods.

Compared to other biometrics

There are a lot of different types of biometric systems. Here’s a high-level comparison of the pros and cons of the most popular ones.

Fingerprint Readers

Fingerprint-based systems are the most common type of biometrics and the most closely associated in the minds of consumers with the industry as a whole. Fingerprint systems work by scanning the tips of one or more fingers and comparing the scans against known images. There are several types of scanning and matching technologies in use today, but the user experience is pretty straightforward: put your finger on a small sensor, wait a second or two for the result.

Advantages:

- Most people instinctively understand the concept of fingerprint scanning, so there's fairly little user training required.
- Fingerprint sensors are quite small, don't consume a lot of power and are becoming inexpensive to manufacture, making it possible to put fingerprint biometric systems on laptops, cell phones, PDAs and even USB thumb drives.
- Fingerprints are the oldest and best-developed sector in the biometrics industry, so there are many vendors and product choices available to the consumer.
- Fingerprint biometric systems have recently become mandated for certain classes of U.S. federal government ID cards, which should spur even more feature development and interoperability among vendors.

Disadvantages:

- Though accuracy has been steadily improving, there is still a real perception that fingerprint scanners are too fidgety for everyday use. This may not be true of most IT applications (where users are conditioned to occasionally repeat required steps), but is a real barrier of physical access control.
- Fingertips are more likely to be dirty than other parts of the body. Dirty fingers can foil the matching process. Dirty fingers also lead to dirty fingerprint readers, which then lead to more poor scans.
- Because many fingerprint systems are not 100% reliable, they are frequently configured with some sort of backup authentication mechanism – such as a PIN number or password - that can be entered in the event that you can't get a good scan. The existence of these backup mechanisms makes fingerprints more useful as a convenience feature, than as an improvement to overall security.
- As a result of a cultural association with criminal proceedings, many people have a strong aversion to having their fingers scanned. This is a significant barrier to widespread adoption in several countries.
- The proliferation of vendors and products has a downside: the fingerprint biometrics industry is rife with incompatible technologies. Interoperability will improve with time.

Applicability:

Today's fingerprint biometric scanners are useful for a wide range of IT applications, but not quite ready for most mainstream physical access uses. The recent growth in demand for fingerprints will likely result in significant overall improvement over the next few years.

Face Recognition

Facial recognition systems look at video or photographs and try to find recognizable facial characteristics and match them against known facial templates to identify individuals. Most current facial recognition system process a 2D camera image, although recent products have emerged that try to map the face in 3D using multiple camera angles.

Advantages

- Anywhere that you can put a camera, you can potentially use a facial recognition system. Many cameras can be installed throughout a location to maximize security coverage without disrupting traffic patterns.
- Face recognition systems can be installed to require a person to explicitly step up to a camera and get their picture taken, or to automatically survey people as they pass by a camera. The later mode allows for covert scanning of many people at the same time.
- Face scanning is non obtrusive, can be done at a comfortable distance and does not require the user to touch anything.
- Video or pictures can be replayed through a facial recognition system for surveillance or forensics work after a security event.

- New 3D facial recognition systems are reportedly showing a surprisingly high level of accuracy and reliability.

Disadvantages

- Accuracy of traditional 2D face recognition systems has been historically poor. Such systems may be fooled by hats, beards, sunglasses and face masks (of the type made popular in international airports during the latest SARS scare.) Even changes of lighting and camera angle can have a significant effect on the accuracy of 2D systems.
- 3D systems, though potentially much more accurate, are still in their infancy. 3D systems will probably also be less nimble at processing large crowds – one of the main advantages of traditional 2D systems.
- Some people view mass-scale facial recognition cameras as the ultimate “big brother” encroachment of security at the expense of privacy. While there are many good arguments on both sides of that debate, potential public distaste for such systems should be considered before implementation.

Applicability

Accuracy rates of facial recognition systems make them poorly suited to making definitive access control decisions, but they are a great supplement to human attention for surveillance applications. Casinos, airports, public spaces and high-security areas can all benefit from some level of facial recognition technology to keep an eye out for known suspects. However, this technology is not yet ready to be the primary method of access control to physical or IT resources.

Hand Geometry

Hand geometry readers study the patterns and angles of an outstretched hand to make a match. The user typical places their hand on a metal plate studded with guide pegs.

Advantages

- Some hand geometry readers are robust and stand up well to frequent use and environmental conditions.
- The actual user interaction with a hand geometry scanner is quick and mostly intuitive.
- The size of a hand geometry “template” (the stored data that’s used to match against the scan) is very small – around 20 bytes – so storing, searching and matching them can be done quickly even on low-end hardware.

Disadvantages

- Hand geometry scanners have to be physically big enough to accommodate an entire, spread out human hand; they’re the size of toaster ovens. This makes the equipment heavy and bulky and therefore only practical in spaces that can physically accommodate them.
- The limited number of data points used by most hand geometry algorithms results in a higher level of false negatives and false positives than some other types of biometrics.
- Some people are squeamish about the sanitary aspects of putting your whole palm in the exact same place as thousands of other people have done before you. There are certainly ways to keep the readers germ-free, but in this age of bird-flu panic, such concerns should not be lightly dismissed.

Applicability

Big, rugged, quick and handy, hand geometry readers are well suited to niche use in warehouses, manufacturing facilities and other industrial locations that have the space to comfortably house them. Hand geometry readers are good for time-and-attendance applications (replacing punch clocks) where their simplicity and rapid cycle times are big assets and their lackluster accuracy rates are not major liabilities. If you put a hand geometry scanner on every door in a typical office hallway, you’ll get an ugly hallway and lots of bruised elbows. Considering that you could cram a dozen cell phones into a single hand geometry reader, don't expect the technology to get much use in consumer products.

Eye Recognition

The eyeball has lots of unique and accessible identifying characteristics that remain fairly constant over an individual's lifetime, making it a potentially ideal source of biometric data. There are two primary places in the eye that are used for biometrics systems today: the retina – the inside back wall of your eyeball, and the iris – the colored disk on the front of the eyeball. A third type, combining aspect of the two as well as other ocular features is called "whole eye". For the purposes of this discussion, we'll treat all three together.

Advantages

- Eye recognition systems tend to be very accurate, with impressively small rates of both false-positive and false-negative errors.
- Iris-based systems are non-intrusive and can be used at a distance of a couple of feet. Using an iris-based system is a bit like looking into a bathroom mirror.
- Unlike with fingerprint readers, virtually all people with healthy eyeballs can be successfully enrolled and scanned with eye-recognition systems.

Disadvantages

- All eye-based systems are a little bit non-intuitive to use. You typically have to stand and look at a certain spot, which can add time to each transaction.
- Retinal systems require shinning a beam of light into the eyeball at a fairly close distance and, even though there's not really any physical discomfort, users sometimes report the same sort of vaguely unpleasant sensations that some people associate with getting an eye exam.
- Until recently, adoption of iris-based systems was hampered by a restrictive patent situation. The patents have recently lapsed, so competition should heat up quickly.
- Quality eye recognition equipment tends to be more expensive today than fingerprint readers.

Applicability

Eye recognition systems show a lot of promise for both physical and IT access control, but the industry is still too immature for mainstream adaptors. The recent lapse of the iris patents should considerably accelerate product development and price erosion of eye recognition systems, so it's certainly worth keeping track of the industry for the next couple of years.

Other Biometrics

There's a plethora of lesser known and idiosyncratic types of biometrics. Hand writing analysis claims to be able to determine your identity by looking at how you physically sign your name. Of course, there's a centuries-old history of handwriting-analysis based quackery, but the current approaches are at least scientifically based and plausible.

Gait recognition tries to identify people by the way they walk. Voice print systems predictably try to identify you by your voice; this would be an elegant approach, but difficulties arise with noisy environments and speech affected by temporary illness. There are even approaches based on body odor and ear shape. A fairly promising new approach is vascular recognition – biometrics based on looking at the patterns of veins visible through the top of your hand. Vascular systems combine the ease-of use of hand geometry with much improved accuracy and smaller readers – plus you don't have to touch anything.

Some of these "alternative" biometric technologies may well prove to be more effective than the common approaches currently in use, but none of them have enough mature products to merit serious consideration for today's mainstream buyer.

Some parting thoughts

In fits and starts, the biometrics industry is starting to catch up to its own hype. Today, this article can only recommend biometrics for surveillance and early-adopter IT applications. If we update this article in the next few years, we hope and expect that our support will be much broader.