The Myth of Fingerprints

By *David Raikow*, Sm@rt Partner
March 12, 2001 11:58 AM PT

Fingerprint readers. Voice-print identifiers. Retina or iris scanners. Face-recognition systems. Those are the things that spy stories are made of. In most people's minds, they are the very essence of high-tech security, and everyone knows that no super secret headquarters worth its salt is without its share of such devices.

But biometrics has extended its reach. It's not just for government agencies and arch-villains anymore.

Reduced manufacturing costs and heightened security concerns have brought a wide array of private-sector companies onto the biometrics playing field, ranging from tiny startups to major industry players like Compaq, Sony and Toshiba. The latest round of marketing places biometrics not merely within your customers' reach, but on the "soon to be a must-have technology" list. According to the hype, the technology improves ease of use and reduces user support costs while securing networks against all but the most formidable attackers.

Those claims are not entirely without merit. Information systems security depends on effective user authentication—the ability to verify that someone claiming to be a legitimate user is who he claims to be. But despite all of the advances made over the past three decades, most networks continue to rely on a centuries old, insecure, user-unfriendly technology: the password. Users hate passwords because they are time-consuming to use and difficult to remember. Security professionals hate passwords because they are easily guessed or stolen. Moreover, the harder it is to steal or guess a password, the harder it is to remember, as well.

Biometric technologies attempt to escape that dilemma by relying on unique physical characteristics, rather than a shared secret, to authenticate users . The system takes an initial set of measurements of the characteristic in question—fingerprint, voice, facial geometry, patterns in the iris or retina—during the user-enrollment process. The measurements are reduced to a template containing data unique to a given individual, but which typically cannot be used to recreate an image or facsimile of the characteristic. Whenever a user needs to be authenticated, the system takes a new measurement and compares it against the stored template; if the new measurement falls within an acceptable range of variation (no measurement is ever exactly the same), the user is granted access.

The authenticating factor is a part of the user's body, so he has nothing to forget or lose. Because the physical characteristics used are highly complex, they can be extremely difficult to falsify, and because they are permanently attached to the user, they can be difficult to steal. The perfect solution, right?

Not so fast. Implementing a biometrics solution involves making fundamental changes to a key element of a functioning network, integrating complex and security-sensitive hardware and software into the existing system, and relying on technologies still in their early-adopter stage. One false move, and your clients could end up paying more to extract themselves from a solution than they did to implement it.

You Are Here Before you head down this road, you need to make sure you have a good sense of where you're starting from; understanding your existing authentication system is essential. According to Jared Beck of biometrics vendor Identix, "People often don't realize that authentication is not just a simple process, but a system that touches most of the pieces of their networks in some way. You have to look at the whole environment, or you'll get yourself into trouble down the road."

The most important element of an authentication system is operating-system access controls. Microsoft, Novell and Unix operating systems each have their own authentication mechanisms and may use distinct methods for managing local and network access; cross-platform networks may use yet another technique for handling authentication between different OSes.

Users accessing a network via dial-in or VPN typically have additional authentication requirements to access an outside ISP, internal modem, and/or VPN gateway. Individual applications often have their own authentication processes, which may in turn include separate local and network elements. Specific network services often have separate processes, as well.

Each of these mechanisms must interoperate smoothly at some level in order to allow access to various network resources. A new biometrics system must take each into account, either to effectively replace, interface with or avoid disrupting them.

Identify Your Target While not entirely inconsistent, the convenience and reduced-support-costs aspects of a biometrics solution place different demands upon the system than do its security aspects. Prioritizing goals is therefore a critical step before the planning process goes into much depth. "Implementation looks very different if you want to maximize short or midterm return on investment rather than your security. If you don't make conscious decisions about trade-offs beforehand, you're likely to get the worst of both worlds," says Jerry Brady, VP of security firm Guardent.

Easy Does It: In addition to relatively intangible benefits to employee productivity, focusing on usability provides definite, concrete advantages. "Help-desk requests to reset forgotten passwords may cost the typical firm $150 to $200 per person, per year," notes Identix executive VP Grant Evans. "A functional biometric system should essentially eliminate that cost. In its first year, a fingerprint system can run as little as $100 per unit, with much of that cost being one-time expenses, so you're looking at regaining your investment in six to nine months."

Those projections assume a large implementation, however. The overall per-unit price point of a given solution will turn on its overall size because of economies of scale in software installation and administration, as well as volume discounts on necessary hardware. While in the midterm, the additional total savings from a large deployment may offset the cost, scalability issues can lead to unexpected problems, and the initial outlay may be prohibitive for many businesses.

The solution's effectiveness in eliminating help-desk costs, meanwhile, turns on its ability to eliminate passwords, at least from the user's perspective. As such, much of the effort of the integration process must focus on integrating the biometric solution with every possible application and service. Every password the user must input is one he or she inevitably will forget, and therefore will be an additional burden on the IT support team. In the absence of consistent standards adoption, this often involves extensive customization and fine-tuning.

A focus on usability also requires a system with an extremely low false-rejection rate; any cost or productivity benefit will quickly disappear if legitimate users are frequently denied access. This is often adjustable via software settings but can impact hardware choices, as well; in any case, lower false-rejection rates can mean higher false-acceptance rates, which can in turn have security consequences.

Watch Your Back: Security-focused businesses, by contrast, can save costs by limiting biometric deployments to specific sensitive accounts, applications and services. According to Chris Klaus, CTO and Founder of Internet Security Systems, "These are often pretty expensive options we're talking about, and people need to ask themselves whether they really need to apply biometric solutions. Usually, they should only be looking at this for their most sensitive assets."

Multifactor authentication is another option that can dramatically improve security. Combining biometrics with passwords, secure tokens, or some other type of authentication can allow different systems to compensate for each other's weaknesses while increasing the sheer number of obstacles for an attacker.

Unfortunately, when it comes to security, many biometric solutions are more flash than substance; implementers must be extremely vigilant to guard against tiny errors or omissions in the implementation process that can all but eliminate most defensive benefits against a proficient attacker. "More often than not, biometrics have very little impact against the really dangerous guys out there. If something slips, they probably won't hurt security, but they probably won't help either," says Guardent's Brady.

Perhaps the most sensitive element of a biometrics system is template storage. Somewhere within your network, the authentication system must maintain copies of these "exemplar" files so that it has something against which it can compare incoming fingerprints, voice prints, iris patterns and the like. An attacker who recovers that data can use it to inject falsified credentials into the authentication process; moreover, once these templates are compromised, they are often extremely difficult to resecure.

Most biometric solutions rely on one or more centralized databases for template storage; this simplifies administration and allows for a concentrated defensive effort. Such databases should always be encrypted; be absolutely certain, moreover, that decryption keys are securely stored and managed. Whenever possible, divide up database fields between separate databases, and encrypt them with separate keys. Be certain that your specific databases have received a thorough security audit, and update that audit regularly.

Some systems permit storage of template files on smart cards rather than networked databases. This approach has a number of advantages—avoidance of a single point of failure, compatibility with off-line and mobile platforms, resistance to remote attack—but are also more susceptible to physical loss or theft. A persistent attacker eventually will recover the template from a stolen smart card.

Solutions designed to include laptops, telecommuter machines and other platforms regularly used while disconnected from the corporate networks often store template files on a local hard drive (the other option being smart-card storage). Such machines are extremely vulnerable and should make use of extensive disk encryption to prevent removal of the hard drive and extraction of data.

In and of itself, biometric data is only designed to authenticate given users, not their local hardware or the servers they access. As such, a solution must incorporate a public key infrastructure (PKI) and encryption protocols to prevent an attacker from tampering with hardware, imitating a client or server, or intercepting communications between them.

Choose Your Allies Carefully According to Raj Nanavati of the International Biometrics Group, "This is still an emerging market, and it's going to be a while before everything shakes out. Until then, picking a vendor will be a tricky business." Moreover, the lack of widely adopted standards makes product evaluation difficult and leaves customers vulnerable to the foibles of individual vendors.

Careful investigation of potential partners is therefore an absolute necessity. Demand detailed information from vendors about their experience with previous deployments, and confirm their answers by chasing down every available customer reference. There's no such thing as a flawless deployment, particularly with such a young technology, so dig deep and get all the dirt on where previous jobs have gone wrong; don't trust anyone who insists their experience has been trouble-free.

Pay particular attention to a vendor's customer-support history and capabilities. A hardware failure or software glitch easily can leave users locked out of their own machines, and vendors should be ready to come to the rescue at a moment's notice. In the same vein, look for firms with significant revenue; a vendor on the verge of bankruptcy is a sinkhole waiting to suck you in.

At this stage in the market's development, it may not be possible to avoid relying upon a specific vendor's hardware, but be prepared to leap on any option that will provide you with interoperability.

Demand that your vendor commit to retrofitting your system once standards are fully developed and adopted. "Right now, this space is far too prone to single-sourcing," warns Identix's Evans. "A lot of vendors are going to disappear, and a lot of customers are going to be left out in the cold."

Proceed With Caution Remember, a pilot program is an opportunity to test and evaluate a potential solution, not simply a prelude to a full-scale deployment. Never trust a vendor's claims regarding performance and error rates; such benchmarks are established under the vendor's ideal conditions, and are almost impossible to evaluate.

"The single biggest mistake in biometrics deployment is the perfunctory pilot program," says Guardent's Brady. "People get entranced with the sexy hardware, and before you know it, the shipping room's knee deep in boxes without any real testing."

Start with a small program that closely approximates your production environment, and then subject it to as much stress as you can muster. Be sure to include every single legacy application you intend to incorporate in your final deployment. Unless you intend to disable all remote access to affected systems, build a VPN gateway or dialup server into the pilot, and test it extensively. If possible, bring in penetration testers to hammer away at your security.

Once you are ready to begin broader deployment, slowly expand your pilot onto production machines. As you expand, scalability issues inevitably will crop up; enrolling and managing 500 users is an entirely different task than enlisting 10 beta testers. Note that some users will be unenrollable due to skin conditions, lost limbs or the like, and have in place an exception-handling mechanism.

Performance and load distribution also may become an issue as the size of the user base increases, so be prepared for a bumpy ride.

In the end, it's up to you to evaluate the risks. The benefits and opportunities are both tempting and very real—but so is the possibility of ending up an early-adoption martyr.

Keep Your Eye/Finger on These

Name	*URL*	*Product*
Ankari	www.ankari.com	BioMouse Sensor
Digital Persona	www.digitalpersona.com	U.are.U Pro
Ethentica	www.ethentica.com	TactileSense T-FPM Fingerprint Sensor Module
Identix	www.identix.com	TouchPrint Live-Scan System
Iridian	www.iriscan.com	Authenticam
Keyware	www.keyware.com	BioGuardians
Polaroid	www.polaroid-id.com	Polaroid PFS-100
Veridicom	www. veridicom.com	5th Sense