

LET'S TALK BIOMETRICS:

A Survey of New Alternatives For User Authentication

By John Prendergast
Veritel Corp.

As the role of computer-related transactions continues to rise in our lives, engineers and designers are re-thinking the user experience. Their objective: to find a better combination of accuracy, convenience, and low-cost for the “user authentication” that is necessary for secure transactions and user confidence.

Today, of course, virtually all authentication revolves around passwords and their numerical counterparts, personal identification numbers (PINs). They are inexpensive and universal, requiring no hardware. Just think about how many different passwords and PINs you use in your own daily life: a password for the corporate network, a PIN for your ATM account, a PIN for your telephone calling card, and a growing number of passwords for the different Web accounts you may maintain for different e-commerce sites.

Unfortunately, passwords and PINs no longer cut it today. While they are inexpensive and universal, the proliferation of these passwords and PINs has created inherent hidden costs and vulnerabilities that are easy for unauthorized users to exploit. For example, many users never change their password from the provided defaults or change them to very obvious words and combinations such as children's names or birthdays. Compounding the matter is the fact that users will typically use the same password or PIN across multiple accounts.

More diligent users might try to maintain separate passwords and PINs for multiple accounts – and maybe even change them on a regular basis. To keep them straight, they'll jot them down on a piece of paper that they keep... near the computer, which defeats their purpose. Or they'll forget the current password, forcing them to call for hints or new passwords – a waste of time and money for all involved.

UNFORGETTABLE: BIOMETRIC AUTHENTICATION

To address these challenges, engineers have begun to seriously examine a more prominent role for biometrics (literally “life measurement”). Ranging from fingerprint readers and palm recognition to iris scans, handwriting recognition, voice recognition, or even DNA analysis, biometrics are based on the immutable truth that no two people are alike -- our fingerprints, voices, eyes, handwriting, and DNA are unique to each of us. And, since computers are excellent at pattern recognition and matching, biometrics offers a compelling avenue for authenticating users.

Of course, most comparisons aren’t perfect matches. Instead, the biometric reading and pattern are compared to the user’s previously recorded biometric and “scored” by the computer. Administrators can then tune the level of security they desire by adjusting the comparison threshold that must be met to authenticate a user.

One of the most important advantages of biometric authentication is that there are no passwords to remember, no cards or tokens to carry, and nothing to lose or steal. Indeed, in a world where biometrics are fully implemented, users would not need credit or ATM cards, nor would they need to sign receipts. Instead, the biometric authentication would reveal and confirm the identity.

Let’s look at the different merits -- convenience, cost, comfort, privacy, and intrusiveness -- for each of the leading “flavors” of biometrics.

Fingerprints

No two sets of fingerprints are alike – as any TV crime-show watcher will tell you. For authentication purposes, fingerprint recognition is the leading biometric method and is appealing because it’s one of the lower-cost options and uses a well-understood, passive process. The user simply puts a finger on a touchpad. The computer then assesses the fingerprint and matches it to a fingerprint it has stored in a database.

Some engineers believe that fingerprint-recognition technology could be built into keyboards and keypads, which means that, for example, corporate-network users could be authenticated as they type. Or ATM users can be recognized as they punch in deposit information.

However, fingerprint recognition has several drawbacks, chief among them false rejection. Touchpads can get dirty quite easily. As a publicly accessible device, it takes abuse ranging from grease and dirt to burrito juice. If the pad isn’t regularly wiped clean, it’s prone to unacceptable error rates.

Fingerprint recognition is also difficult to implement in certain devices, such as mobile phones, where form factor limitations make it unfeasible.

Pal mprint Recognition

Similar to fingerprint recognition, palmprint recognition asks the user to place his hand on a “palm reader” as a means of authentication. However, instead of comparing prints, palmprint recognition measures the user’s unique “hand geometry” and compares it to previously captured and stored measurements and ratios of users’ hands.

Of course, these pads are vulnerable to the same types of drawbacks: public abuse through constant touching. User reluctance – an unwillingness to put a hand on a public device – tends to be higher than with fingerprint recognition. Also, the form factor is larger, driving up costs.

Iris Scanning

Perhaps less well-known, the human iris is no less unique than a human fingerprint. In an iris scan, a simple optical scanning light shines on the human eye and compares it to previously a recorded scan. The iris scan provides a highly reliable and highly secure means of authentication.

But the obstacles to widespread adoption of iris scanning are significant. The first is a cost issue. Few iris-scanning devices have been deployed widely for authentication because of their relatively high cost. Another impediment is user resistance. To the uninitiated, an iris scan can provoke reactions ranging from hesitation to outright fear. Although the scan is very safe and is performed much like a flatbed scanner or fax machine, users worry that “a laser beam” is going to cause eye damage. Given their cost and usability issues, iris scans have largely been confined to high-security applications where they’re used in combination with other security measures.

Face Recognition

Combining the visual measurements of iris scanning with the geometric calculations of palmprint recognition, face recognition optically measures the contours of the user’s face and compares the unique angles and measurements. Unfortunately, this combination provides a “worst-of-all-worlds” result. It’s expensive to implement, users are reluctant to have their faces scanned, and false rejections are unacceptably high.

Other strategies exist – such as taking a pin-prick blood sample and comparing the DNA with previously recorded samples. However the safety risks, intrusiveness, and high cost eliminate these types of options from any feasible

mass-market deployment. Of course, some of these biometrics have other drawbacks. For example, physically challenged users cannot use prostheses for fingerprint or palmprint recognition. Cost and “Big Brother” issue of intrusiveness remain key hurdles for design engineers to address.

VOICE VERIFICATION: NOW YOU’RE TALKING

The one biometric that can rapidly ramp up to rapid adoption – through both lower cost and increased user acceptance -- is **voice verification**. In “voice recognition,” the computer merely recognizes what was said. However, “voice verification” does not determine the message content. It verifies the identity of the speaker based on prior samples of that individual’s speech, usually by using a predefined text phrase. The basic steps are:

- **Enrolling** -- The customer speaks the defined phrase (such as “Your voice is your password.”).
- **End Pointing** – The computer must find the beginning and ending of the phrase. This process is the foundation on which other analyses take place, so it’s critical to get it right. Leading technologies use a technique based on the amount and timing of energy in the signal.
- **Frame Analysis** -- Within each 30 ms “frame,” you can find well-formed, regular patterns that are as unique as fingerprints. These patterns are created by the size and shape of the physical structure of the vocal tract. A “Linear Predictive Coefficient (LPC) Cepstral Analysis reduces the frames to a set of numbers that represent the physical characteristics of the speaker.

This numeric information is a “signal reference file.” Typically, one signal reference file is not enough information about a person’s voice. It’s a good strategy to capture two or three signal reference files from users. Collectively, these files become the user’s voiceprint. During verification, the new rendition of the defined phrase (“Your voice is your password.”) is compared with the voiceprint on file and scored for its similarity, creating a confidence ranking that administrators can tune to their desired threshold. Newer technologies – called “Fine Measurement” can analyze even smaller 4-8 ms segments of speech -- such as vowel sounds – for even greater accuracy and confidence.

There are several advantages to voice verification as a biometric authentication technology. Perhaps most important is that the infrastructure for voice is already in place. While few fingerprint readers are out in the market today (to say nothing of iris scanners), virtually every PC today ships with some type of microphone and sound card. For entry-level systems or older PCs, after-market microphones and cards are available in virtually any computer/electronics retailer.

They're a stable, proven, low-cost technology that's already supported by most leading computer operating systems. And of course, mobile phones are ideally suited to voice verification as the most intuitive method for user verification. That means voice verification is ideal for corporate network security, mobile-phone applications (e.g. to prevent cell cloning), and even Web security and verification for banking, e-commerce purchases, account access, and more.

Technically, voice verification is appealing as well. A speech print (at 11 KHz) consumes only 8-10 kilobytes and an average Pentium III server can process 200 verifications per second. Voice is also a less intrusive biometric. The user needn't touch anything or submit to intrusive optical scanning – just say a 1-2 second phrase.

Of course, voice has its minor drawbacks as well, with laryngitis posing the greatest obstacle. In voice verification, losing one's voice is equivalent to losing one's password. A person's voice does, indeed, change over time, so periodic renewals of the voiceprint – perhaps every 12-18 months – can reduce false rejections.

Identical twins are another challenge because of their similar physical structures. However, impersonation is not a risk because a computer does not "listen" as a human does. George Bush needn't worry that Dana Carvey can clean out his bank accounts.

CONCLUSION

The type of biometric you select for user authentication should properly depend upon the application you have. A government weapons facility easily justify a combination of biometrics (and other authentication techniques as well, such as passwords and access cards) while those techniques would be inappropriate for accessing the corporate network.

In the future, biometrics will combine with digital signatures for non-repudiable authorizations and authentications that will support the billions of business transactions that have to date relied on physical signatures.