Why I Love Biometrics
It’s “liveness,” not secrecy, that counts.

BY DOROTHY E. DENNING

I’m a big fan of biometrics. I’m tired of trying to remember umpteen zillion account names and passwords in order to use the computers in my office, browse my favorite Web sites and update the Web sites I manage. I long for the day when computers will automatically recognize me and handle the identification and authentication function with little effort on my part.

I make lots of security-related presentations, and when I tell all of this to an audience, someone inevitably asks, “What happens if someone snatches the biometric print used to validate you? Couldn’t they just replay your biometric and pretend to be you? Wouldn’t that make your biometric as good as useless?”

My response is, “No.” A good biometrics system should not depend on secrecy. To understand why, think about how biometrics work in the physical world. Your friends and colleagues authenticate you by recognizing your face, voice, eyes, hands, gait and so on. None of this is secret. Anyone who interacts with you sees these characteristics. Even your fingerprints can be lifted from surfaces.

What makes biometrics successful is not secrecy, but rather the ability to determine “liveness.” I can easily distinguish the living, flesh-and-blood you from a statue or photograph of you, or even someone wearing a costume and mask that looks like you. If I don’t know you well, I might be fooled by a lookalike, but in the non-*Mission Impossible* real world, the system generally works. If I don’t know you at all, I might ask for a photo ID. But I would use such a photo only because I lack knowledge of your appearance. I authenticate you by comparing your live face against the photo, not by comparing one photo against another. For further proof, I may watch you sign your name and compare the live signature against the one on your ID card.

The same principle applies in the digital world. Your biometric prints need not be kept secret, but the validation process must check for liveness of the readings. Many biometric products work this way, and I would like to see product surveys tell me which do and do not. The iris recognition system from **Sensar (www.sensar.com),** for example, looks for the “hippus movement” -- the constant shifting and pulse that takes place in the eye. The liveness test ensures that the reading is fresh, so an adversary can’t replay a previously recorded reading.

This is the beauty of biometrics. Other forms of user authentication--including passwords, tokens and encryption--all depend on protecting a secret or device from theft. Once that secret or device is compromised, the system fails until a new one is established. Moreover, these methods typically require users to hold a different secret with each and every device or service they use, thereby burdening the user. Imagine if every time you greeted a friend or colleague, you had to provide a different secret password!

Testing liveness is reasonably straightforward if the biometrics reader senses appropriate characteristics and is tightly coupled with the validation process and database of biometrics prints. If the reader is remote from the validation process and database, encryption can be used to provide a secure path connecting the components. The encryption system, obviously, should protect against replays. Encryption can also be used to pass credentials from one system to another. For example, once my smart card validates my fingerprint, it may use a private signature key on the card to authenticate me to services that use my public key for authentication. Of course, the encryption system itself requires secret keys, but in this context, the secrets may be less prone to compromise because they don't have to be known by humans.

Biometrics can be applied not only with human users, but also with locations. For example, technology from CyberLocator (www.cyberlocator.com) authenticates geodetic location by capturing a location signature from GPS signals in a way that ensures liveness. No secrets are required. One could imagine using biometrics to authenticate places or anything else with distinguishing characteristics that exhibit a form of liveness.

In addition to liveness, a biometrics system also depends on uniqueness. Otherwise, it may be subject to false accepts or rejects. Some forms of biometrics are better than others in this regard, iris recognition being one of the best.

Questions about privacy abuse aside, biometrics is likely to be the way of the future. I can't wait to get rid of my gazillion passwords and sticky notes.

DOROTHY E. DENNING, Ph.D., is a professor of computer science at Georgetown University and a member of *Information Security*'s Editorial Board.