

Inside Risks 110 (*CACM* 42, 8, August 1999)
Biometrics: Uses and Abuses
Bruce Schneier

Biometrics are seductive. Your voiceprint unlocks the door of your house. Your iris scan lets you into the corporate offices. You are your own key. Unfortunately, the reality isn't that simple.

Biometrics are the oldest form of identification. Dogs have distinctive barks. Cats spray. Humans recognize faces. On the telephone, your voice identifies you. Your signature identifies you as the person who signed a contract.

In order to be useful, biometrics must be stored in a database. Alice's voice biometric works only if you recognize her voice; it won't help if she is a stranger. You can verify a signature only if you recognize it. To solve this problem, banks keep signature cards. Alice signs her name on a card when she opens the account, and the bank can verify Alice's signature against the stored signature to ensure that the check was signed by Alice.

There is a variety of different biometrics. In addition to the three mentioned above, there are hand geometry, fingerprints, iris scans, DNA, typing patterns, signature geometry (not just the look of the signature, but the pen pressure, signature speed, etc.). The technologies are different, some are more reliable, and they'll all improve with time.

Biometrics are hard to forge: it's hard to put a false fingerprint on your finger, or make your iris look like someone else's. Some people can mimic others' voices, and Hollywood can make people's faces look like someone else, but these are specialized or expensive skills. When you see someone sign his name, you generally know it is he and not someone else.

On the other hand, some biometrics are easy to steal. Imagine a remote system that uses face recognition as a biometric. "In order to gain authorization, take a Polaroid picture of yourself and mail it in. We'll compare the picture with the one we have in file." What are the attacks here?

Take a Polaroid picture of Alice when she's not looking. Then, at some later date, mail it in and fool the system. The attack works because while it is hard to make your face look like Alice's, it's easy to get a picture of Alice's face. And since the system does not verify when and where the picture was taken—only that it matches the picture of Alice's face on file—we can fool it.

A keyboard fingerprint reader can be similar. If the verification takes place across a network, the system may be insecure. An attacker won't try to forge Alice's real thumb, but will instead try to inject her digital

thumbprint into the communications.

The moral is that biometrics work well only if the verifier can verify two things: one, that the biometric came from the person at the time of verification, and two, that the biometric matches the master biometric on file. If the system can't do that, it can't work. Biometrics are unique identifiers, but they are not secrets. You leave your fingerprints on everything you touch, and your iris patterns can be observed anywhere you look.

Biometrics also don't handle failure well. Imagine that Alice is using her thumbprint as a biometric, and someone steals the digital file. Now what? This isn't a digital certificate, where some trusted third party can issue her another one. This is her thumb. She has only two. Once someone steals your biometric, it remains stolen for life; there's no getting back to a secure situation.

And biometrics are necessarily common across different functions. Just as you should never use the same password on two different systems, the same encryption key should not be used for two different applications. If my fingerprint is used to start my car, unlock my medical records, and read my electronic mail, then it's not hard to imagine some very insecure situations arising.

Biometrics are powerful and useful, but they are not keys. They are not useful when you need the characteristics of a key: secrecy, randomness, the ability to update or destroy. They are useful as a replacement for a PIN, or a replacement for a signature (which is also a biometric). They can sometimes be used as passwords: a user can't choose a weak biometric in the same way they choose a weak password.

Biometrics are useful in situations where the connection from the reader to the verifier is secure: a biometric unlocks a key stored locally on a PCM-CIA card, or unlocks a key used to secure a hard drive. In those cases, all you really need is a unique hard-to-forge identifier. But always keep in mind that biometrics are not secrets.

Bruce Schneier <schneier@counterpane.com> is President of Counterpane Systems. You can subscribe to his free security newsletter, CRYPTO-GRAM, at <http://www.counterpane.com>.