Biometric authentication

Kurt Seifried, kurt@seifried.org

Biometrics have garnered increasing attention and backing in the last few years. We are promised a utopian existence: never again will you forget your password or need to remember your access card to get into the building. Unfortunately, it isn't quite this simple. While biometrics will be a significant portion of any authentication or identification in the future, they cannot replace many existing security systems without significant disadvantages. Using biometrics in conjunction with other proven security methods can result in a stronger solution; but using biometrics on their own is a very bad idea, for numerous reasons.

Breaking Biometrics

Like any security system, a biometric system can be compromised. While many vendors make compelling arguments against just this issue, it isn't unthinkable. Fingerprint scanning systems (and by extension hand geometry readers) are relatively old and can be based on any number of technologies, from simple optical scanner to lasers, sonar, pressure-sensitive pads, and so on.

Of these systems optical ones are probably the most vulnerable. Because they rely simply on a camera to take a picture of the ridges and bumps on your fingers, you can fake some out with a simple black and white picture of a person's fingerprints. For others, a latex mold of the finger is needed — a task that is far from being impossible.

Newer systems actually use a mechanism such as a laser to read the actual surface of your finger, generating a detailed three-dimensional map that can also detect the presence of a pulse. Some go so far as to check for body heat. Hopefully companies will choose a technology that is extremely hard to fake out. For cost reasons, however, many will likely go with cheaper optical solutions and the like.

The next step up would be using the eye as a source of identification. Many systems utilize the blood vessel pattern on the back of the eye, and some use features contained in the iris. These systems are much harder to defeat, but it is only a matter of time before someone can develop a sufficiently advanced fake eyeball that fools detectors.

These systems also face some difficult acceptance problems. People are afraid to stick their eyes up to something that has a laser in it — never mind that this laser cannot put out enough power to damage the eyeball. I personally have had laser eye surgery (Lasik in both eyes at the same time), and I am still somewhat leery of sticking my eye up against something that can scan it.

Voice recognition systems are also becoming popular. Unlike the first two, they do not require you to stick your finger or eye into anything, and they are extremely easy to use ("Please repeat the following sentence"). Numerous difficulties exist, though, since people's voices change constantly: we get colds, get laryngitis, we mature over the years, and so forth.

Voice generation is still sufficiently difficult that it will not be possible for some time to generate another person's voice very well. And recording someone's voice can be countered rather simply by requiring the user to repeat a random phrase or list of words.

Camera-based systems show promise. Not only can they recognize your face, but if attached to your workstation they can automatically log you out when you go to the bathroom and log you back in once you return. These systems vary from simple optical scanners to combinations of optical and infrared (and possibly other wavelengths in the future). In theory, someone with a good latex mask and wig should be able to fool these systems out; infrared makes it more difficult, but probably not impossible. This is another kind of system that is extremely easy to use (please look at the camera for a moment).

Despite all these wonderful technologies, one simple problem looms. At some point (probably sooner than we hope) attackers will find ways to spoof your finger/eye/voice/face. Then the question is, how do we fix it? Does the company upgrade all of its biometric scanners to models that cannot be faked out? Or, like the credit card companies, does it simply pass the cost of fraud on to consumers in the form of higher rates?

The Dishonest Merchant

Skip forward 20 years. You're at the store paying for groceries. You slide your smartcard into the machine, mash your thumb on the pad and hit the large green Accept button. Money is automatically moved from your account to the merchant's, and all seems well.

Unfortunately, what you didn't notice is that the merchant has made modifications to his fingerprint reader. Instead of just scanning your thumb and using that to unlock the smartcard, it has also recorded your thumb. Now, if the merchant can get ahold of your smartcard, they can access it and clean out your account.

This is currently possible with debit cards. It would be reasonably trivial to make a fake keypad that records people's PIN numbers. And since the debit card is just a simple magnetic strip, it is possible to copy this strip when the card is swiped, and load the data onto another card.

We haven't heard of much fraud of this type, however. The number of people with debit card machines is restricted to merchants, so if someone were to try this, it would become quickly apparent who had the modified machine. However, as the use of debit cards increases, we can imagine someone building a fake vending machine. For example, you select what you want, feed it your card and type your PIN in. This is all recorded, and then the machine declines the transaction.

The above has happened in the past with fake ATM machines, but because of their limited use, it is relatively easy to track down. What happens when every single purchase we make uses a debit card or some newer alternative?

The Solution?

Like any system, biometrics can be hardened and more layers of security added, but this of course costs significant money. If we had smartcards that need a thumbprint to unlock them, then putting the reader on the card would solve many problems. But this is bound to be more expensive than just rolling out smartcards and giving merchants the thumbprint readers.

Use of strong PKI could help prevent replay attacks and fake machines that try to get you to put in your PIN or give up a thumbprint. If every merchant terminal had a unique individual certificate signed by a trusted authority (such as the bank), and your smartcard had the bank's public key and a red and green LED light to let you know if the certificate was legitimate or not, then fake terminals would be far more difficult to set up.

Using multipart authentication, a token plus a thumbprint plus a PIN number, greatly increases the survivability of a system. But these solutions cost money, and if credit cards are any indication, then merchants and consumers seem willing to foot the bill for fraud.

Back

Last updated 4/10/2001