Digital dangers: do biometric solutions offer a false sense of security. (Biometrics).
Joe Grand

09/01/2002
e-Business Advisor
62

ADVISOR REALITY CHECK

Long thought to be the strongest of security solutions, it's been discovered that **biometric** devices do have their flaws.

THE GENERAL PUBLIC'S EXPERIENCE with **biometrics** is largely limited to what they've seen in the movies. The big-screen hero approaches a top-secret, secured room and encounters a **biometric** scanning device ... that he promptly defeats with some clever trick. However, as most technical folks know, **biometric** technology isn't fiction anymore--and unfortunately, neither are methods for faking them out.

Biometric technologies measure and analyze human body characteristics to authenticate identity. Fingerprint scanning is currently the most pervasive **biometric** technology. Other traits detected with **biometric** solutions include hand geometry, eye pattern (iris or retina), facial features, voice signature, written signature, and keyboard patterns. The devices measure the **biometric** characteristic, record it into a digital file, and compare it to aversion stored in a secured, trusted back-end database.

The first commercial **biometric** device was installed at a Wall Street firm more than 25 years ago, so the concept is far from new. Most **biometric** systems are used today as absolute identification to control and monitor access to a physical facility or data. The system must be able to separate a known person from the universe of unknown people with more reliability than an intelligent, attentive human screener.

Biometric dangers

A **biometric** system is composed of two or three components:

* A **biometric** device--such as a fingerprint scanner, camera for facial recognition, or voice recognition hardware--that connects to a host PC or workstation.

* Application software or middleware running on the host.

* A trusted back--end server. This option is often used for large-scale, enterprise wide deployments. In some situations, the application software handles the authentication and the back-end server isn't used.

Each component of the system has specific security risks and potential points of failure. Modification or manipulation of a fingerprint, disguises or face-obscuring hairstyles, or changes in iris characteristics caused by taking certain medications can affect the accuracy and

reliability of the system. Insecure design of the ***biometric*** *reader hardware could let an* attacker retrieve internal or secret data components. An attacker could also obtain digital credentials representing a user's **biometric** by monitoring network traffic between the various connections. A flaw at any stage could result in user information being leaked and misused.

Although **biometric** measures are generally considered to be more secure than systems that use passwords, the physical characteristics that **biometric** systems use are hard, if not impossible, to keep secret. An attacker can lift a fingerprint from a keyboard or doorknob, take a picture of a face, or simply record a voice. Compare that to a password or PIN a user can memorize.

If you use your voice as a **biometric**, it can be compromised if an attacker records your voice or obtains the digital file containing your voiceprint from the reader or back-end server. After a **biometric** is stolen, it should be considered insecure forever. Changing your voice isn't as easy as changing a password. This situation holds true with fingerprints, as well; but you have ten fingers to choose from before you run out of options. Some systems claim to store only a small sample of data instead of the complete fingerprint, so if one sample is compromised, you could use the same finger again with a different sampling technique. However, this small sample may reduce the uniqueness of the fingerprint, making absolute identification more difficult.

It also may not be safe to assume that the human characteristic being relied upon for authentication will always remain the same. Although some traits, such as retina geography, usually stay [the same over the course of a person's lifetime, scars on a finger, minor changes in an adult's voice, or loss of a linger or eye in an accident, can hinder the effectiveness of the **biometric** solution. The latest crop of glaucoma medicines can change the color and vein pattern of the retina, which can also be true of corrective laser eye surgery.

Failures and inaccuracies of **biometric** systems are another major point of controversy. For example, in January 2002, the American Civil Liberties Union proved that face recognition software employed by the Tampa, Florida police failed to identify one single criminal or suspect listed in the department's photographic database over four days, while falsely identifying 14 innocent citizens. The system was abandoned after one month of use.

Gummy fingers

At the May 2002 ITU-T Workshop on Security in Seoul, South Korea, Tsutomu Matsumoto presented experiments and methods to defeat a number of fingerprint scanners by using a fake finger molded out of gelatin. The goal of Matsumoto's work was to test the accuracy of fingerprint scanners. Using "**gummy**" fingers easily made of gelatin with common tools and materials, he defeated 11 different fingerprint scanners 80 percent of the time.

It was known before Matsumoto's experiments that creating a silicone rubber mold from a real human finger could fool fingerprint scanners using optical sensors (the majority of currently available devices, in which light is bounced off the finger and retrieved and processed by a detector). Fingerprint scanners using a capacitive sensor (a matrix of sensors detects minute changes in electrical capacitance on the human finger, which corresponds to bumps and ridges) usually reject the silicone rubber molds. Because a gelatin finger has moisture and resistance characteristics similar to a real human finger, Matsumoto's **gummy** finger fooled both types of scanners.

It's unclear if Matsumoto's fake fingers will work on some of the newer fingerprint scanning technologies, for example, those that use low-level radio frequency (RF) transmissions to image the fingerprint structure in lower layers of skin. Because the gelatin finger is just a thin layer, the sensor would probably reject the fingerprint. Obviously, Matsumoto's attacks should be recreated and tested on RF-based scanners before they're considered reliable.

The importance of Matsumoto's work lies not only in the simplicity of the attack, but in the alarmingly high, 80-percent success rate. Although fingerprint scanner technologies have been available for years, only now has publicly released research shown faults. Chances are that other **biometric** technologies have undiscovered or undisclosed faults, and it's only a matter of time until they, too, become weakened or broken.

A thumbs down for **biometrics**?

In a world where you should use different passwords for different systems, **biometrics** prevent this by relying on a single **biometric** trait as the password. If a **biometric** is compromised, a piece of the user's identity is therefore compromised. However, **biometrics** may be suitable in certain situations. A reasonable situation would be for a **biometric** to be used for authentication purposes to a stand-alone laptop or desktop for home or personal use. Relying solely on **biometrics** for identification and access to a classified government research facility, for example, is unacceptable.

Companies that have already implemented a **biometric** security solution should scrutinize their systems to ensure proper storage of credentials and correctly implemented encryption and communication protocols between all components. Another good strategy is to layer the technology with other security solutions. For example, you could use a hardware-based, one-time-password or authentication token along with the **biometric** technology.

Be aware that introducing another layer of security also introduces another layer of risk because of the communication points between the layers. However, having a multiple-factor solution with something the user knows (password), something they have (hardware token), and something they are (**biometric**), should definitely help reduce the chances of unauthorized access.

Joe Grand is an independent consultant and electrical engineer specializing in product design and development. His pioneering hardware research has been published in various academic and industry journals. He has lectured widely on security product analysis, portable devices, and digital forensics. Previously, Joe was a co-founder of digital security consulting firm @stake.