Letters

To the Editor:

While I enjoyed the excellent special section on biometrics in the February issue, I was alarmed that the authors did not point out a serious security problem with this approach.

While described as an advantage, the fact that a biometric signature cannot be changed introduces a security risk for many applications. In the digital world, once a digital representation of a biometric signature is compromised, an imposter can use it in the same way as a PIN or password if the entire system is not totally secure. The examples described in the articles that involve networked systems are at least as difficult to secure with biometrics as with more conventional passwords. In fact, if the representation of the biometric signature is large, a secure initial connection is more computationally difficult to achieve and may discourage its use.

In defense of biometric approaches, applications such as access control to a restricted area where the user presents identification to an offline and physically secure system, this risk may be minimized (although not totally eliminated).

At a minimum, I would be reluctant to allow the use of my biometric signature for access to a networked system unless I have high confidence that the remainder of the system is secure. At least for a password-based system, I have the security of knowing that the password can be changed if or when it is compromised.

Paul Losleben
Palo Alto, Calif.
losleben@snf.stanford.edu

The guest editors respond:

Before discussing their loss or compromise, we need to precisely define biometric identifiers or signatures. If a biometric identifier is a physical body characteristic such as a fingerprint, it can’t be lost short of losing the body part. However, the record of a biometric signal or signature can be compromised if this piece of digital information somehow falls into the wrong hands.

We do not believe that an imposter can use a compromised biometric signal or signature in the same way a thief uses a stolen PIN or password. First, the biometric signature is probably encrypted, and the imposter must discover the decryption key. The recorded biometric signature then has to be fed into the system somehow, bypassing the sensor. Using techniques like hiding data in the authentic biometric signature, smart sensors, and challenge response systems can make such manipulation very difficult.

In addition, thieves or impostors would have to doctor the hardware, which is not the case for password-protected systems. Thus, while the sensor level is an admittedly vulnerable point of attack for biometric systems, all other points of attack are the same as in password or PIN systems because, in essence, the access control system architecture is the same.

We strongly feel that biometrics will deter and prevent fraud in mass-market point-of-sale applications. For credit card transactions, where merely possessing a credit card is accepted as proof of identity—for example, at a gas pump—any means of identity authentication will diminish fraud.

We do agree, however, the security aspects are grossly neglected in many biometric applications. What we need is for security experts to start looking more seriously at the area of biometrics.

Changing the SeC Focus from Processes to People

To the Editor:

It has always amazed me that software capability evaluations (E. O’Connell and H. Saiedian, “Can You Trust Software Capability Evaluations?” Feb. 2000, pp. 28-35) usually focus on the organization’s processes and almost never evaluate the training, experience, and talent of its personnel.

I have seen organizations in which people who have never had a course in computer science have produced considerable paper trails with Microsoft Project and Visual Source Safe. They, therefore, demonstrate their maturity in project management and configuration control even though they can’t produce working code. In this regard my grandmother qualifies as a project manager through her excellent system for filing recipes and planning meals.

It’s time to address the taboo of never asking or requiring information about how well prepared people are to produce software. Does an organization employ software developers with academic degrees in computer science/engineering? How many years of experience in developing software do these people have and what have they produced? Can they pass a standardized computer science/engineering test?

While it won’t solve all contractor problems, I do think it’s time to apply such questions and tests. Even postal workers undergo greater scrutiny than software developers.

David Cox
North Chili, N.Y.
dcox1@rochester.rr.com

A Must-Read for Program Managers

To the Editor:

The software capability evaluations article by Emillie O’Connell and Hossain Saiedian is a must-read for DoD program...