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 imposters 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 SFC 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 Emilie O’Connell and Hossain Saiedian is a must-read for DoD program managers. 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.

Letters
Fooling the Team Is Tougher Now

To the Editor: Emilie O’Connell and Hossein Saiedian have pointed out significant problems with the present state of software capability evaluations. As one who has been involved in several SCEs, I appreciate their candor.

It is true that one outcome of an internal SCE (which can be conducted by an external organization under contract) is a maturity level score. However, when the acquisition agency follows the SCE 3.0’s recommendation and tailors the process to meet its needs, the SCE may not produce a level rating. Even when the process covers the entire model, some acquisition agencies may not want or need a level rating. Instead, they try to evaluate the risks associated with the bidder under evaluation. While this is a commendable goal, it often degrades into the assignment of a “meets requirements” rating to all of the evaluated contractors.

On the other hand, acquisition organizations may use the threat of an SCE to limit the number of bidders. Because the acquisition process is expensive for both the bidders and the government, limiting the evaluation to the bidders who can tell up front whether or not they meet the basic qualifications can be a good thing.

A few years ago, it may have been possible to fool an SCE team. But now, some acquisition agencies are hiring consultants from companies that specialize in conducting SCEs. Fooling these experienced teams is more difficult, and it may be impossible.

Despite the problems, imposing the CMM and SCE processes on government contractors has had a positive impact. Contractors will do whatever their customers want (and will pay for). If they don’t improve their software processes, they won’t be competitive and will have to find other work. In the long run, I think these processes will succeed in eliminating poor practices. However, until we settle on the best way to develop software, SCEs may still be necessary to prevent backsliding.

Roy Kimbrell
O maha, N eb.

Revisions Improve SCE Processes

To the Editor: I read “Can You Trust Software Capability Evaluations?” with great interest. However, I am concerned that this article might add to the confusion about SCEs for readers who are not familiar with the subject.

The authors refer to the 1987 SEI Maturity Questionnaire, which was replaced in 1994 (CMU/SEI-94-SR-7). In addition, they did not refer to the current SCE method, Version 3 (CMU/SEI-96-TR-002). Version 3’s most important feature is that it complies with the CM M appraisal framework, which the SEI developed to make appraisal results compatible for both a CM M-Based Appraisal for Internal Process Improvement (CBA IPI) and SCE.

Both the DoD and the federal government now allow contractors to “reuse” SCE results if the SCE meets certain conditions. For example, the SCE must have been conducted within a designated timeframe, and the evaluation must have been conducted by the organization that is bidding for the current opportunity. This means that the government realizes that these evaluations pose a burden for both the contractors and the selection teams.

Boris M utafelija
G elmantown, M d.
bmutfelija@hns.com

The authors respond:

The intent of our article was to point out the flaws in the application of SCEs and to discuss how those flaws allow the DoD software crisis to continue.

We do not believe the SCE method is at fault. Rather, both the evaluating acquirer and the contractor introduce problems. These problems are fostered by a lack of understanding and improper application by the SCE team, as well as an “us versus them” audit mentality that leads to misrepresentation by the contractor.

M r. M utafelija correctly points out the changes in the maturity questionnaires, RFP templates, and permissibility of SCE reuse. We agree that many SCEs are conducted properly and will effectively protect the government acquirer from underqualified contractors. However, the examples in our article demonstrate that in spite of its merits, the SCE technique does not guarantee such protections.

Since our article was published, we have received a number of “confessions” from contractor personnel attesting that our observations are not uncommon.