The authors respond:

Our analysis of the relationship between speculative fiction and real-world technology focused primarily on 20th-century fiction but, given space, we could have gone back much further than Swift—to Augustine’s City of God, for example, or even to Plato’s Republic.

We disagree with the suggestion that Swift’s machine ought to be credited as an “early attempt at artificial intelligence.” For those unfamiliar with Swift’s work, this machine was actually a room filled with students who randomly pulled wires to mix up a large set of words stuck to wooden plates. The students then wrote down any phrases that emerged from this random churning. The students’ professor intended to piece these phrases together “to give the World a compleat Body of all Arts and Sciences.”

From our perspective, this machine is satire—as is much of Swift’s work—and as such can hardly be credited as either a progenitor of artificial intelligence or as being influential in the history of computing.

BIOMETRIC IDENTITY THEFT
To the Editor:

In the otherwise excellent special section on biometric identification in the February 2000 issue of Computer, several authors emphasize how biometric measures cannot be lost, forgotten, or misplaced. But this convenience comes at a cost: If they are in fact lost, biometric identifiers cannot be revoked and new measures reissued. Passwords can be changed or digital signatures can be replayed undetectably into the system’s authentication modules using Trojan horse or virus software or the signature acquisition on biometric identification as such can hardly be credited as either a progenitor of artificial intelligence or as being influential in the history of computing.

Continued from page 4

Letters

The authors respond:

Our analysis of the relationship between speculative fiction and real-world technology focused primarily on 20th-century fiction but, given space, we could have gone back much further than Swift—to Augustine’s City of God, for example, or even to Plato’s Republic.

We disagree with the suggestion that Swift’s machine ought to be credited as an “early attempt at artificial intelligence.” For those unfamiliar with Swift’s work, this machine was actually a room filled with students who randomly pulled wires to mix up a large set of words stuck to wooden plates. The students then wrote down any phrases that emerged from this random churning. The students’ professor intended to piece these phrases together “to give the World a compleat Body of all Arts and Sciences.”

From our perspective, this machine is satire—as is much of Swift’s work—and as such can hardly be credited as either a progenitor of artificial intelligence or as being influential in the history of computing.

BIOMETRIC IDENTITY THEFT
To the Editor:

In the otherwise excellent special section on biometric identification in the February 2000 issue of Computer, several authors emphasize how biometric measures cannot be lost, forgotten, or misplaced. But this convenience comes at a cost: If they are in fact lost, biometric identifiers cannot be revoked and new measures reissued. Passwords can be changed or digital signatures can be replayed undetectably into the system’s authentication modules using Trojan horse or virus software or the signature acquisition on biometric identification as such can hardly be credited as either a progenitor of artificial intelligence or as being influential in the history of computing.
Letters

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 sce 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...