Interface

Identifying security enhancements

Dear Editors,

I agreed with several of the points and examples in the article "The Assault on Logic" (Privacy Matters, July/Aug. 2003), but I feel that author Michael A. Caloyannides also missed the point in several places and used the same misapplication of logic he attempted to debunk to prove some of his arguments.

I agree that security is not synonymous with identification, but there is a clear and basic relationship: coupling identification with a way to authenticate it can be a crucial factor in ensuring security. Strictly speaking, the author is correct that knowing who every person is walking down every street doesn't promote security. The key, however, is rather to be able to verify anyone's claimed identity for any specific purpose. The ability to identify someone is separate from determining when it's appropriate to do so. How to do it should be based on technological and economic issues; when to do it should be based on law and policy as related to the consequences of not doing it.

Caloyannides argues that having identified the participants in the 9/11 attack wouldn't have prevented the attack because none of the men were on watch lists. Yet his logic is flawed—we now know that several of them should have been on various lists; knowing who they were at times such as when they entered the country or took flying lessons could have gone a long way toward preventing the attack.

I agree that an over-robust identification system can lull us into a false sense of security, but this doesn't mean it shouldn't be part of the toolkit. To prevent the perception that identification verification provides total security on its own, we must also educate and inform.

Identification and verification would actually help prevent the negative results described in many of his examples in the section on slander and misinformation. For example, knowing the true source of a report can go a long way toward determining its credibility. This doesn't mean the public, or even the government, has a right to know that source, but identity and identity verification help to create accountability.

The author further discusses data mining's inability to prevent terrorism. Using the Oklahoma City bombing as an example, he says that a system looking for people renting trucks and buying fertilizer would have flagged most of the farmers in Nebraska. The question then becomes whether the perpetrator was currently engaged in farming. If not, a cross-reference of nonfarmers renting trucks and buying fertilizer might have raised a danger flag for law enforcement. Furthermore, if a repository had been available that allowed information analysis, authorities might have determined that the persons renting the truck and buying the fertilizer didn't own or lease land or farm equipment, hadn't recently purchased other associated supplies or equipment, and weren't employed by someone that did satisfy such criteria. However, most of this discussion is moot because those who rented the truck and purchased the fertilizer used false identities to do so. Perhaps a robust method of identity verification would have come in handy?

At the end of his column, Caloyannides advocates purposefully providing misinformation when you know that someone (a government or your estranged spouse's lawyers) is scrutinizing your actions. Yet, doing so when you know that the recipient is a law enforcement agent executing a properly authorized warrant could very well be illegal.

Privacy issues often bring about responses based on emotion and politics rather than logic. We should be more concerned with who has access to information and the purpose (both intended and collateral) for which the information is used. We need to develop a system of checks and balances that provides rules for information use and imposes significant consequences for misuse or failure to provide adequate protections to prevent unauthorized disclosures.

—Stan Bush
srbush@nps.edu

Michael A. Caloyannides responds:

Mr. Bush reaffirms my position that identification enhances security in connection with access to data and facilities, but not in "knowing who every person walking down the street is."

Concerning the 9/11 tragedy, however, he argues that because some of the perpetrators were on watch lists—for a traffic violation in Florida in one case, an expired visa in another (an illegality shared by millions of illegal aliens in the US)—a check of such lists could have gone a long way toward preventing the attack. But the old "connecting the dots" argument doesn't work when there are as few dots to connect as in this case. A record of past petty crime and some pilot training could hardly indicate something as shocking as that someone would hijack an airplane full of innocents and fly it into a building.

Continuing on the unsubstanti-

ated premise that identification somehow creates security from terrorism, Mr. Bush argues that, despite some concerns, an "over-robust identification system" should be part of the security toolkit; this argument is seductive in its simplicity, but it fails to assess the vast problems introduced by deploying such a system—namely, the strong likelihood and historical precedent for abuse.

Mr. Bush argues in favor of database mining, suggesting that it might have flagged the McVeigh purchases in Oklahoma City. Yet, a savvy would-be terrorist could negate such techniques through basic operational stealth—by befriending a farmer to purchase the fertilizer, for example. Furthermore, the US Congress recently assessed the pros and cons of such database mining (in the form of DARPA's Total Information Awareness effort) and summarily dismissed it by eliminating the funding and directing that it be cancelled.

Finally, Mr. Bush suggests that we should promptly assist all law enforcement agents. But what if he were living in Idi Amin's Uganda (or any of the numerous other countries under totalitarian rule) when a law enforcement agent handed him a "properly authorized warrant"? Would he feel motivated to assist in such a charade of legality if faced with the risk of being executed as the reward for compliance? Respect for legal authorities and the laws they enforce is predicated on the premise that both have legitimacy. That, in turn, derives from being in a free society where the laws represent the will of the people through their elected representatives, and enforcers are accountable for their conduct.

Leading the way with policy

Dear Editors,

I'd like to thank Marc Donner for another engaging column, "Deus Est Machina" (Biblio Tech, July/Aug. 2004), and adding to my reading list. I'm pleased to see that both *S&P* and *IEEE Spectrum* gave consideration to science fiction (and Vernor Vinge) in July as sources of insight into the challenges our profession will face.

My only point of difference is in the conclusion. As a matter of ethical considerations and enlightened self-interest, we must actively initiate and carry on the dialogue within our profession, with policy makers, and with a broader public community. As your column suggests, most fiction focuses on technology's dystopian implications (necessarily, because "nice" doesn't sell), which means the public gets only these perspectives from popular entertainment (the movie *I, Robot* [based on the book by Isaac Asimov] is a recent example). If we leave the policy-making to the political folks and a misguided public, the outcome will not be ideal.

Too few of our members take up the challenge of a proactive role in the policy dialogue. The IEEE Society for Social Implications of Technology (SSIT), IEEE-USA, the IEEE Professional Activities Committee for Engineers (PACE), and some activities in other "jurisdictions" (Canada and Europe) provide paths in this direction. The IEEE Computer Society also maintains a TechnoPolicy email list for discussion of related items at www.computer.org/tab/technopolicy/.

We still have an opportunity to get ahead of the game to be seen as leaders rather than reactionaries.

—Prof. Jim Isaak
j.isaak@snhu.edu

How to Contact *IEEE Security & Privacy*

Writers

Visit www.computer.org/security/author.htm or log onto Manuscript Central at http://cs-ieee.manuscriptcentral.com/. Authors must use Manuscript Central to upload their submissions. First-time users must create a new account.

Letters to the Editors

Send letters to Kathy Clark-Fisher, Lead Editor, kclark-fisher@computer.org. Please provide an email address or daytime phone number with your letter.

On the Web

Access www.computer.org/security/.

Subscription Change of Address (IEEE/CS)

Send change-of-address requests for magazine subscriptions to address.change@ieee.org. Be sure to specify *IEEE Security & Privacy*.

Subscribe

Visit www.computer.org/subscribe/.

Missing or Damaged Copies

If you are missing an issue or received a damaged copy, contact membership@computer.org.

Reprints of Articles

For price information or to order reprints, send email to security@computer.org or fax +1 714 821 4010.

Reprint Permission

To obtain permission to reprint an article, contact William Hagen, IEEE Copyrights and Trademarks Manager, at copyrights@ieee.org.