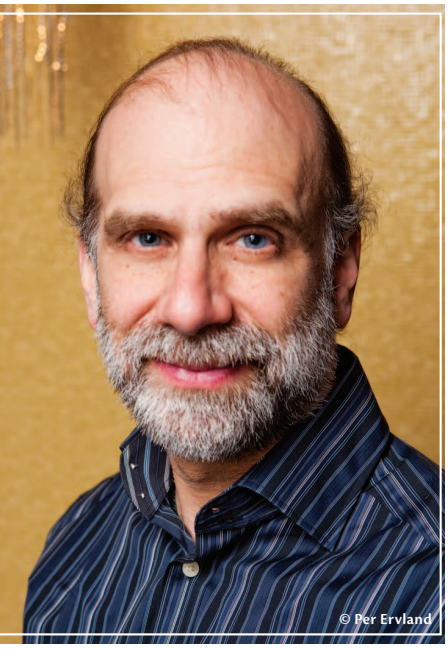

The Importance of Security Engineering

Bruce Schneier
BT

In May, neuroscientist and popular author Sam Harris and I debated the issue of profiling Muslims at airport security. We each wrote essays, then went back and forth on the issue. I don't recommend reading the entire discussion; we spent 14,000 words talking past each other. But what's interesting is how our debate illustrates the differences between a security engineer and an intelligent layman. Harris was uninterested in the detailed analysis required to understand a security system and unwilling to accept that security engineering is a specialized discipline with a body of knowledge and relevant expertise. He trusted his intuition.

Many people have researched how intuition fails us in security: Paul Slovic and Bill Burns on risk perception, Daniel Kahneman on cognitive biases in general, Rick Walsh on folk computer-security models. I've written about the psychology of security, and Daniel Gartner has written more. Basically, our intuitions are based on things like antiquated fight-or-flight models, and these increasingly fail in our technological world.

This problem isn't unique to computer security, or even security in general. But this misperception about security matters now more than it ever has. We're no longer asking people to make security choices only for themselves and their businesses; we need them to make security choices as a matter of public policy. And getting it wrong has increasingly bad consequences.

Computers and the Internet have collided with public policy. The entertainment industry wants to enforce copyright. Internet companies want to continue freely spying on users. Law enforcement wants its own laws imposed on the Internet: laws that make surveillance easier, prohibit anonymity, mandate the removal of objectionable images and texts, and require ISPs to retain data about their customers' Internet activities. Militaries want laws regarding cyberweapons, laws enabling wholesale surveillance, and laws mandating an Internet kill switch. "Security" is now a catch-all excuse for all sorts of authoritarianism, as well as for boondoggles and corporate profiteering.

So what do we do? We need to establish security engineering as a valid profession in the minds of the public and policy makers. This is less about certifications and (heaven forbid) licensing, and more about perception—and cultivating a security mindset. Amateurs produce amateur security, which costs more in dollars, time, liberty, and dignity while giving us less—or even no—security. We need everyone to know that.

We also need to engage with real-world security problems, and apply our expertise to the variety of technical and socio-technical systems that affect broader society. Everything involves computers, and almost everything involves the Internet. More and more, computer security *is* security.

Finally, and perhaps most importantly, we need to learn how to talk about security engineering to a nontechnical audience. We need to convince policy makers to follow a logical approach instead of an emotional one—an approach that includes threat modeling, failure analysis, searching for unintended consequences, and everything else in an engineer's approach to design. Powerful lobbying forces are attempting to force security policies on society, largely for nonsecurity reasons, and sometimes in secret. We need to stand up for security. ■

Bruce Schneier is the chief security technology officer of BT. His latest book is *Liars & Outliers: Enabling the Trust that Society Needs to Survive* (www.schneier.com/lo). He can be found online at www.schneier.com.

Copublished by the IEEE Computer and Reliability Societies
1540-7993/12/$31.00 © 2012 IEEE