Back in the July/August 2006 issue of IEEE Security & Privacy, the editors of the Book Reviews department wrote an essay entitled, “Why We Won’t Review Books by Hackers.” They argued that to review such books would be to “tacitly endorse a convicted criminal who now wants to pass himself off as a consultant.” We published two letters to the editor in the subsequent issue, and that was the end of the topic. Or so you thought.

In this issue, I argue that whether S&P reviews them, you should read the writings of bad guys, with the usual caveat that you should do so if they have something useful to say and are well written. This topic has been debated for many years, and the positions boil down to one of four basic arguments:

• The writings of bad guys are morally tainted.
• We should not reward bad guys for bad behavior.
• The writings of bad guys provide “how to” information for the next generation of bad guys.
• The writings of bad guys glamorize bad behavior and should be eschewed along with other attractive nuisances (to steal a term from the legal community).

If the moral taint disqualification fails for Mein Kampf, then there’s no reason we should let it stop us reading the works of lesser criminals. Fundamentally, any writing that gives the good guys an insight into the behavior of the bad guys is useful.

In the case of black hat computer adventurers, there’s no legitimate employment, so a book’s economic importance to the bad guy might be quite significant. On balance, however, this is a red herring. Negligibly few books are so popular that they change the fortunes of their authors. Most books have no more than modest success that, in the best case, produces a few hundreds or perhaps thousands of dollars for the author. This isn’t enough to make a real behavioral difference. Moreover, if a book becomes incredibly successful, it’s likely that the book’s value to society outweighs the harm that comes from rewarding the bad guy. A more subtle argument is that bad guys write books to market their skills for later employment as security experts. This argument is similarly bogus because it’s really “moral taint” in disguise. Without getting into an imponderable debate on ethics, this argument comes down to the assertion that a bad guy can never be reformed and that skills learned from bad behavior should never be used for gain.

The third argument—that bad-guy writing passes evil skills on to future bad guys—falls apart similarly on deeper analysis. It reduces to the old security through obscurity chestnut, which our community has been on the forefront of rebutting. Besides, cybercrime is a fast-paced arms race, and most of last week’s tools and techniques are ineffective and irrelevant this week. Of course, the more general techniques that bad guys use to develop attacks are as valuable to defenders as they are to attackers.

The last argument (about attractive nuisance) is an interesting one. The world of cybercriminal-authored books clearly breaks into two parts—those whose authors have been caught and convicted and those whose authors have not. All the bad-guy books I can think of have been written by convicted criminals. Books written by unconvicted criminals lack a certain—to put it delicately—credibility, wouldn’t you say? After all, it’s hard to believe that an uncaught and unconvicted bad guy would reveal all the vulnerabilities he knew. And if you want to trade time in jail and the permanent status of a convicted criminal for the dubious chance at fame that writing a true cybercrime book brings, then you probably already have severe problems.

Most fundamentally, however, the department editors noted that the book they were refusing to review was uninformative and badly written. This makes the book a waste of time by violating my rule that bad-guy books should be “useful and well written” to be worth reading. So if you hear about a good book by a bad guy, by all means read it.