Free Software Matters: Security Through Freedom

Eben Moglen*

June 15, 2002

Software security is all the rage this year, for predictable reasons. It's hard to talk about public policy with respect to software, at least in Washington, without talking about security. For Microsoft, continuing its attack on free software and the GNU General Public License in particular, security is the new favored place to attempt to undermine the free software movement.

The spokesmen for this attack, however, have been third parties, rather than Microsoft itself. This, in my opinion, reflects the increasing caution Microsoft feels after its disastrous claims last summer that the GPL is a "cancer" or a threat to the American way of life. Better to have someone else say the aggressive things that may not be justified; if they're said by some "reputable" third party they can always be quoted in your own propaganda later on.

Enter the Alexis de Tocqueville Institution [www.adti.net], an "independent" think tank with a variety of free market interests, and a variety of funders, including, as it happens, Microsoft. On May 30, the Institution released a "report" arguing that free software, which it calls "open source" software, shouldn't be used by governments because it is easier for terrorists to attack computer systems whose source code they can read and understand.

As I have written here before [ref to column in Apr01?], one of Microsoft's biggest vulnerabilities in maintaining the unfree software monopoly is the possibility that governments around the world will decide to

*Eben Moglen is professor of law at Columbia University Law School. He serves without fee as General Counsel of the Free Software Foundation. You can read more of his writing at http://moglen.law.columbia.edu.

stop buying unfree programs they can't understand, can't modify or improve, and can't redistribute—spending, worldwide, tens of billions of dollars annually of their taxpayers' money on programs whose free software equivalents they could have for next to nothing. Finding reasons for governments to avoid free software is difficult: free software is a typical "public good," about which economists can give lots of reasons for government support to production, and very few reasons against. In the most literal sense, free software is the public's business. But, says the Alexis de Tocqueville Institution, that would help the terrorists destroy national security.

Another threat to the Western Way of Life? No, just hogwash. This report is a classic example of the belief in "security through obscurity": make your systems secure by not telling people how they work. And, as experts have been trying to tell business and government for decades, security through obscurity just isn't secure at all.

The first problem is that such security is only as good as the obscurity itself. Is Microsoft Windows secure because only a few tens of thousands of people around the world have access to the source code? That's probably not the best guarantee that no one will figure out its weak points. Indeed, security through obscurity is useless for a more general reason: "crackers," the break-in artists and electronic smash-and-grab thugs who populate the darker corners of the net, don't need the source code to find problems with programs. The classic way of attacking the security of computer programs is to feed them unexpected and deceptive inputs and watch what happens: use very long responses to test for buffer overflows, use unexpected inputs to test for holes in verification routines, etc. Windows has not been trouble free for security specialists, after all, because it was so easy for virus builders and other black-hat programmers to stress test their way to knowledge of the system's vulnerabilities.

Free software is, in fact, far more secure than proprietary software, for the same reason that it has fewer defects of other, non-security kinds. First, the entire user community is able to read the code and locate problems through static analysis; problems are unearthed as people learn about the programs for their own purposes. And when problems are recognized, through any means, they can be fixed by the first person who discovers them. So fixes are quicker to attain, and can be vetted, in turn, by thousands of users around the world immediately. And third, the resulting improved versions of the program can be distributed in the decentralized, non-hierarchical way that all free software is distributed: no waiting for everyone to download a binary patch from the Microsoft website.

Within days of the release of the Institution "report," all of these points had been made by security specialists, and the press was beginning to inquire who had paid for the study in the first place. The Institution refused to specify, but Microsoft admitted that it provides money to the Institution. Another campaign of fear, uncertainty, and doubt had blown up on the launchpad. Back to the drawing board once again, no doubt.

Just a silly little attempt by the monopoly to get its dirty work done at second hand? Yes, but if you think about it, there's a deeper lesson. It's the one we've all been trying to learn in the democratic societies since September 11. The best protection for the security of our societies is freedom itself, which isn't a source of weakness but rather a source of strength. Despotism and unfreedom achieves only, as one American Supreme Court Justice once wrote, the unanimity of the graveyard. Freedom protects freedom, which is why—in our "new" world of ever-present security concerns—Free Software Matters.