



Code on the Internet Battlefield Needs Body Armor

By Peter Coffee
September 18, 2006



eWEEK.com Special Report:
Securing the Network

Opinion: Reverse engineering is both a tool of attackers and an instrument of national policy.

Continued controversy over U.S. military spending makes it a useful allegory of issues that arise in allocating IT resources. In the same way that defense planners find billions for high-tech systems but fall short in simple tasks like armoring soldiers, IT planners may be constructing vast new server farms that offer up key intellectual property as a much too easy target.

It's hard enough to protect mere data in customer-facing systems: eWEEK Labs has shown, in four international hacking challenges, that there's a worldwide community of knowledgeable experts with both the tenacity and the access to online resources that are needed to find and exploit database vulnerabilities. Much more hazardous are the systems that expose applications, or actually download executable code, to client devices and their users.

"Releasing .Net and Java applications without obfuscating them is tantamount to distributing the source code," observed Senior VP Sebastian Holst at Preemptive Solutions in response to one of my columns earlier this year—and as I said in that column, failing to take reasonable protective measures may be tantamount to yielding ownership rights. Yes, Holst has a dog in this fight: His company produces source obfuscation tools. That doesn't mean he's wrong, as anyone can independently determine by aiming any of several free decompilation tools at a company's code base.

Moreover, any issues of protecting intellectual property become even more complex as international markets become the major opportunities for sales growth—and also major centers of potential competition in commercial software development. I spoke last week with one software development executive who preferred not to have her company named, saying that there's no advantage to be gained in defying potential attackers to take them on: "We found international companies that do reverse engineering and aren't really prevented from doing that," she said, and "We found companies whose technology has been cracked and you can get the unblockers online; we found other companies whose solutions required compilation of their code into the executable, which would affect our release schedules."

This conversation points up the role of reverse engineering, not just as a tool of attackers, but as a matter of national competitiveness. Some have argued, for example, that recent antitrust actions against Microsoft in Europe are the migration into the courtroom of a war that couldn't be won in the laboratories.

These developments shine the spotlight on today's announcement by **V.i. Laboratories** of Waltham, Mass., of that company's CodeArmor 2.0 technology for adding reverse-engineering protections to executable code. My conversations with V.i. developers and with the above-quoted customer of the company suggest that the product addresses an intimidating portfolio of possible attack modes, including some that I'd never before considered involving code crackers' use of sophisticated emulation environments.

As I've previously observed, nothing is too hidden to hack, but the V.i. Labs customer that I interviewed last week was realistic about that. "It's a lock on the door," she said. "It won't last for 10 years, but it will protect something for as long as it takes us to put out our next release in six months." That's a realistic perspective on a critical need for anyone whose code has to go out there and fight for a living