[in]security

by Gary McGraw

Is Cisco Naked? : : :

The only way we're going to start doing security right is by deeply understanding software exploits. We can't pretend that modern analysis tools such as disassemblers don't exist. Nor can we pretend that some kinds of software (say, router software) are immune to hard-core analysis. The story of 26-year-old Michael Lynn should drive this point home.

WHAT COLOR IS YOUR HAT?

Up until the Black Hat conference in Las Vegas this July, Michael Lynn was employed by Internet Security Systems (ISS) as part of its X-Force team of security researchers. He was scheduled to give a talk entitled "Cisco IOS Security Architecture" at the conference. The abstract said it would "provide an architectural overview of IOS and explore the feasibility of code execution against Cisco routers." This is the very code that runs most of the routers on the Internet. In his talk, Lynn was to describe a way to build software exploits that would work against existing bugs. (That's right—the bugs are there for the 'sploiting.) Cisco was all set to help with the talk.

Interestingly, Cisco knew all along of security bugs very similar to the ones Lynn was to discuss and had even released patches to fix at least one of them. But it didn't spend enough time looking for more. These bugs are a symptom of a bigger problem—the problem of insecure software.

Just before the talk, ISS and Cisco decided that some of the content was too dangerous to disclose—actually, they said that disclosure would be "premature." They even went to great lengths to quash the presentation. Cisco employees physically removed the 20-page presentation out of the conference materials and destroyed more than 2,000 CDs containing a copy of it. (Of course, the presentation is all over the Internet now.) ISS, Cisco, and Black Hat also agreed that Lynn would present an alternative talk on a different subject.

But Lynn himself didn't agree. Instead, he resigned his position at ISS and went on to cover parts of his original presentation. Unfortunately, much of the technical meat of the talk was removed. The slides had even been changed.

THE EMPEROR IS NAKED

Whatever Lynn presented was enough to get him in hot water. Cisco and ISS together sought a federal court order barring him and Black Hat from any further dissemination of what they said was their proprietary information. According to Cisco and ISS, Lynn crossed the line of standard vulnerability disclosure when he gave the talk. Cisco had warned Lynn in no uncertain terms not to talk about how he reverse-engineered the IOS code. But security problems don't cease to exist just because they're not talked about. Lynn didn't put the bugs in the Cisco code.

Instead of focusing its corporate time and energy on finding and removing security problems in its products, Cisco went after a 26-year-old kid with all its legal firepower. This is a crying shame and a disservice to security. Perhaps we'll have to rewrite *The Emperor's New Clothes* and adjust the ending. In the new version, the little boy will get thrown in jail so that the Emperor can remain blithely and happily naked.

> "Instead of removing the security problems in its products, Cisco went after a 26-year-old kid."

So the question is, is that good for security? Do we really want companies to censor security-critical information like this just because it makes them look bad? I think not. Cisco and other companies need to do a better job with software security.

If you're a Cisco customer, you should pressure your vendor to produce more secure software. Tell the folks there to spend their time clothing the Emperor (that is, building more secure products) instead of throwing the little boy in jail.

Gary McGraw is CTO of Cigital, a software quality management consultancy. He is co-author of *Exploiting Software* (Addison-Wesley, 2004), *Building Secure Software* (Addison-Wesley, 2001), and *Java Security* (Wiley, 1996). Reach him at gem@cigital.com.