A Security Technologist's View

Bruce Schneier discusses the Sklyarov Case and the DMCA

On 16 July in Las Vegas, the FBI arrested a Russian computer security researcher, because he presented a paper on the strengths and weaknesses of software used to protect electronic books. Because of the Digital Millennium Copyright Act (DMCA), which makes publishing critical research on this technology more serious than publishing nuclear weapon design information, Dmitry Sklyarov (age 27) landed in jail. Just how did the United States of America end up with a law protecting the entertainment industry at the expense of freedom of speech?

I've already written about the DMCA, and the futility of employing technical solutions to prevent digital copying. The specific DMCA provision at work here is the one that explicitly forbids the invention and distribution of "circumvention devices" and "reverse engineering of document protection." Basically, it is illegal to break--or show how to break--technology used to protect digital copyright. If you do, you go to jail (see above).

Technically, the law only protects "effective" copy-protection technology. This is a wonderful piece of circular logic: surely if is has been broken, then it wasn't effective. The complaint against Sklyarov sidestepped this problem: "Nevertheless, because the book sold in encrypted form and only accessible through the eBook Reader and is not duplicatable, the copyright holder's interest in the book is protected." But if that were true, then there would no grounds for the case.

There are also provisions in the DMCA to allow for security research, provisions that I and others fought hard to have included. But these provisions are being ignored, as we've seen in the DeCSS case against 2600 Magazine, the RIAA case against Ed Felton, and this arrest.

What the DMCA has done is create a new controlled technology. In the United States there are several technologies that normal citizens are prohibited from owning: lock picks, fighter aircraft, pharmaceuticals, explosives. (Ignore guns, since the 2nd Amendment makes it impossible to generalize from their example.) In each of these cases, only people with the proper credentials can legally buy and sell these technologies. The DMCA goes one step further, though. Not only are circumvention tools controlled, but information about them is. 2600 Magazine merely described and linked to implementations of DeCSS. Ed Felton wanted to present a paper on the deficiencies of the RIAA's various watermark schemes.

I attended Dmitry Sklyarov's talk at DefCon. What he did was legitimate security research. He determined the security of several popular E-Book reader products and then notified the respective firms of his findings. His company Elcomsoft published, in Russia, software that circumvented these ineffectual security systems. His DefCon talk was a clear and evenhanded presentation of the facts. He said, in effect: "This security is weak, and here's why." (One particular company he mentioned stored the password in plaintext inside the executable. So, anyone with Notepad and a few minutes of scrolling could have the book modified for easy distribution.)

The FBI nabbed him at the request of Adobe Systems, Inc. for breaking the security on Acrobat's E-Reader API, and held him without bail.

In 1979, "The Progressive" magazine tried to publish an article containing technical information on H-Bomb design. The government claimed publication of this article would result in "grave, direct, immediate and irreparable harm to the national security of the United States."

After six months of legal manoeuvring, they published it. In 1971, the government tried to prevent "The New York Times" from publishing "The Pentagon Papers." The Supreme Court promptly voted 6-3 to reject the government's censorship attempt, with chief Justice Warren Burger declaring that "prior restraints on speech and publication are the most serious and least tolerable infringement on First Amendment rights."

Welcome to 21st Century America, where the profits of the major record labels, movie houses, and publishing companies are more important than First Amendment rights.

In many ways, we're seeing the legacy of the NSA's long war against cryptography and cryptographic information. Until the late 1990s, the NSA used the threat of national security to prevent the dissemination of encryption technologies. When they could, they blocked the publication and dissemination of information. When that failed, they concentrated on products, using both legal and illegal methods to block encryption software. Many people believe the NSA's primary rubric, export controls, would not stand up to a constitutional challenge, but it was never tested. The NSA eventually gave up.

During those debates I was often asked about the NSA's strategy. Wasn't it doomed? Yes, it would eventually fail. But from the NSA's point of view, every day they could delay the failure was a day of victory. Maybe the Export Control regulations (they were never laws) were unconstitutional. Maybe preventing publication of this and that was prior restraint. Maybe pressuring companies to install back doors into their software was illegal. But if it worked for a while, it was a win. The NSA was fighting a holding action, and they knew it.

The entertainment industry is behaving in the same way. The DMCA is unconstitutional, but they don't care. Until it's ruled unconstitutional, they've won. The charges against Sklyarov won't stick, but the chilling effect it will have on other researchers will. The entertainment industry is fighting a holding action, and fear, uncertainty, and doubt are their weapons. We need to win this, and we need to win it quickly. Please support those who are fighting these cases in the courts: the EFF and others. Every day we don't win is a loss.

Copyright 2001 Bruce Schneier <schneier@counterpane.com>