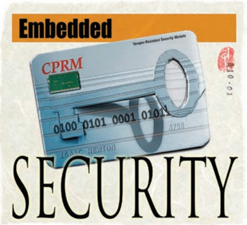
COVER FEATURE

Copy Protection Technology Is Doomed



Those determined to bypass copy-protection technologies have always found ways to do so—and always will. A copyright holder's best protection lies in creating an attractive business model.

Dan S. Wallach
Rice University

At some fundamental level, seemingly as axiomatic as the speed of light or the conservation of energy, copying information—strings of bits—will always be easy. Historically, systems intended to restrict this fundamental property have always been defeated, and there is no reason they won't continue to be defeated.

Copying has always been easy, whether it was my junior high school computer buddies running Copy][+ to pirate games in our school's computer lab or kids today swapping MP3 files on Internet chat systems and burning them to CD-ROMs. But vendors continue selling content and people continue to buy it, even when they can get that content illegally.

HISTORICALLY UNFOUNDED CONCERNS

Copyright concerns have persisted for as long as the media for making copies have existed. Some early musicians refused to record their work, fearful that nobody would attend their live shows. When radio appeared, record companies feared that it would cannibalize record sales. These fears never materialized. Instead, with analog music technology, copying music always entailed generational loss. For that matter, every time you played a record, the quality declined as the needle wore down the record's surface. To have the best fidelity, consumers would purchase their own copies. Radio play served as an advertisement for consumers to buy record albums, which in turn created fans to attend live performances. Existing copyright law proved quite sufficient to shut down attempts to produce pirated copies.

The introduction of the compact disc initially *reduced* music piracy because duplicating CDs required expensive equipment and because CDs provided features not available with analog technology, such as instant track skipping and improved resistance to wear and harsh environments. Because CDs were a fundamental advance over earlier analog technology, consumers had less incentive to copy digital music to analog media.

SNAKE-OIL CURES

With the ubiquity of CD burners, technology has again advanced, making copying audio CDs bit for bit trivial. The record companies could address this situation by creating fundamental advances in how they deliver music to consumers. Instead, technology companies are offering the record companies a wide variety of snake-oil schemes to help them maintain their previous business models. These schemes *can* be defeated—doing so only requires that somebody study how they work.

Watermark woes

Some copy-protection systems focus on watermarking music by adding largely inaudible distortions to it before the content reaches the consumer.

Watermarks can encode digital information, whether they are as simple as a single bit—"this music is or is not copyrighted"—or as complex as the purchaser's user ID. Likewise, watermarks can be either *fragile* or *robust*. Even modest changes in the music generally destroy fragile watermarks, whether by converting from digital to analog and back, or through a lossy compression scheme like MP3—which compresses audio by removing sounds inaudible to most listeners.

Robust watermarks are engineered to survive these transformations. Some schemes use a robust watermark to identify a tune's original purchaser. If that tune later appears in wide distribution, the purchaser could be held liable for damages. Imagine the reaction if a record company dragged a 13-year-old girl into court because she gave her friends a track from the latest boy band.

0018-9162/01/$10.00 © 2001 IEEE

Other schemes combine a fragile watermark with a robust one to indicate two bits. The robust watermark's presence indicates that a copyright protects the music, while the fragile watermark indicates the music is still in its original form. Every CD player, computer sound card, and music-reading or -playing device in the world would be required to detect these bits. If a copyrighted song had been tampered with, the device might refuse to play it. If a song remains in its original form, it might then be subject to some kind of security policy, perhaps a rule that only "compliant" devices can handle the track and that these devices allow making only a few copies before deleting the original.

Not a bit safe

Rather than focusing on watermark schemes—which have all been defeated, anyway—devices such as digital-audiotape drives and other more recent systems simply embed copy-protection bits in the metadata. If the bits say "this is a first-generation copy," the device might allow creation of a backup labeled "second generation" but might disallow backups of the second-generation copy.

These schemes only work when device manufacturers uniformly follow the standard. Once a deviant device becomes available, or existing devices' firmware has been reverse-engineered and suitably modified, these bits become merely advisory and can be casually ignored. The movie industry discovered this phenomenon when the freely available DeCSS software tool, using information reverse-engineered from a normal DVD playback package, chose not to follow the rules.

Even in a world of truly uniform devices, such as game consoles or satellite TV receivers, these schemes are still easily defeated. The Sony PlayStation provides a great example. The PlayStation stores its games on standard compact discs, but Sony arranged for some tracks to have invalid checksums. No self-respecting CD burner would ever write invalid checksums, so the PlayStation only needs to validate that the checksums are, in fact, invalid to abort the game-loading process.

It's easy to defeat the PlayStation's protection system by using a low-cost embeddable microprocessor and soldering a few traces onto the PlayStation's motherboard. The new chip watches the host computer as it reads data from the CD. When it sees a request for the invalid block, it clocks out the invalid data to the host computer, regardless of what is on the CD. You can download code for these chips for free, or you can ship your PlayStation to vendors who will "chip" it for a small fee.

Revocation schemes

Some vendors propose a revocation scheme in which all shipped content would include device-specific cryptographic keys. When hacking instructions appear online, subsequent content releases would delete the cryptographic keys for the hacked device. Consequently, future content releases would not play properly on these devices. The vendor would then be forced to replace confused consumers' once-working devices. Alternatively, consumers could reverse-engineer the device-specific keys from some other device and install those keys inside their device.

Further, once pirates have extracted the necessary secrets, they can program their PCs to perform the decryption, yielding unencrypted content that they can easily share over the Internet or via other means. Laws that might restrict commercial companies from producing such software will have little practical effect on the free-software community.

Devices such as digital-audiotape drives and other more recent systems simply embed copy-protection bits in the metadata.

IP WANTS TO BE FREE

Rather than giving up, the snake-oil salesmen now seek to buttress their broken technologies by leveraging the legal system, using various combinations of patent law, trade secrecy, and new laws that ban reverse engineering. These new laws, including the Digital Millennium Copyright Act in the US and comparable laws elsewhere, make a farce of free-speech rights and of essential legal balances like the right of fair use. Pending US legislation, including the Security Systems Standards and Certification Act, might actually mandate that all content-playing devices have "certified security technologies." Might the US government ban Linux? Hopefully, the SSSCA will be withdrawn and challenges against the DMCA will succeed.

History tells us that the ease of digitally copying music, video, and any other media won't destroy the copyright holders. It also tells us that attempts to restrict copying will uniformly fail. The only way to prevent teenage girls from freely sharing boy-band MP3s will be to provide reasonably priced service that's irresistibly better than free file sharing. Some vendors, such as eMusic.com, are beginning to offer flat-rate subscription services that appear to be a step in the right direction. Any other technology, business model, or legal framework is simply doomed. ✷

Dan S. Wallach is an assistant professor at Rice University. His research interests include a variety of security topics. Wallach received a PhD in computer science from Princeton University. He is a member of the IEEE, the ACM, and Usenix. Contact him at dwallach@cs.rice.edu.