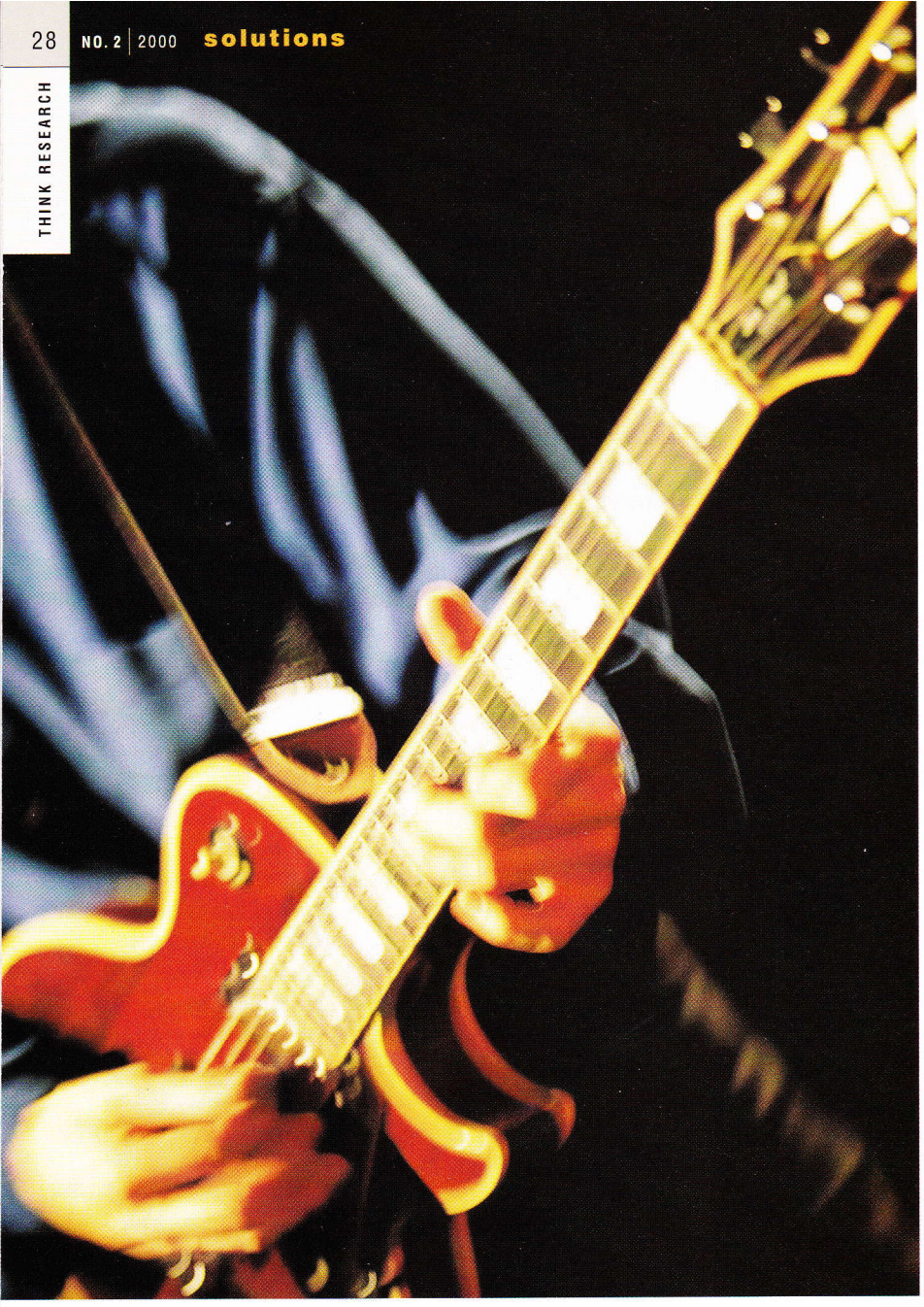
think research
IBM LEADERSHIP THROUGH SCIENCE AND TECHNOLOGY



WEB TECHNOLOGY

CHAINED MELODIES / BY JOHN LEHMANN-HAUPT

THE ABILITY TO REPLICATE AND TRANSMIT digital audio files with absolute fidelity is revolutionizing the distribution of music. At the same time, however, it's creating a major headache for the music industry. "In the last year and a half or so, the industry has been hit by two developments," says Jeffrey Lotspiech, a research staff member at IBM's Almaden Research Center. "The first is low-cost recordable CDs and recording drives, and the second is MP3 — the protocol for compressing music files so that they can be easily distributed on the Internet."

With the help of free software provided by Napster, Inc., which makes possible the location and unrestricted downloading of any desired song in the personal computer libraries of all of its users, MP3 has become so popular among students that stores in college and university towns have already reported dramatic decreases in sales volume. Although the Recording Industry Association of America is already engaged in legal proceedings aimed at obtaining an injunction against Napster for copyright infringement, similar systems are emerging that are less centralized and may prove even harder to pursue through legal recourse.

"It is of paramount importance to the music industry that it acquire the means to offer the consumer an equally convenient, yet legitimate, alternative to Napster-style services through online retail outlets, but with full copy protection," says Alan Bell, director of digital media standards and commercialization at Almaden. "Without the technology to ensure compensation to creators and distributors, there will be little motivation to continue to produce new music."

And now, with the imminent debut of DVD (Digital Versatile Disc)-Audio, the industry has even more at stake. DVD-Audio is a new disc medium with the capacity to offer either two channels of superhigh fidelity sound (24 bit sampling at a rate of 192 kHz, compared to the CD standard of 16 bits at 44.1 kHz) or up to six channels at a sound quality still better than CD. Although the DVD format dates back to 1995, when Bell was instrumental in bringing together competing companies to avert a dual-format debacle like the VHS/Beta video wars of the 1980s, it has to date seen service primarily as a highly successful medium for movie purchase and rental.

As a major source of technology for furthering all forms of e-business, IBM has contributed to many areas of Internet security and protection of intellectual property. For the DVD-Audio

launch, IBM — in conjunction with Intel, Matsushita and Toshiba (collectively known as the "4C") — has devised a new protection scheme based on encryption, called Copy Protection for Prerecorded Media (CPPM). When authorized by the copyright owner, the same basic technology may also be used in "secure" versions of portable MP3 players, which began to appear on the market this summer.

The heart of these new protection systems is a way of encrypting the content so that it can be decrypted only by a compliant playback device. The IBM/4C scheme is also designed to control the limited copying of prerecorded DVDs that the recording industry, unlike the movie industry, is willing to allow. The owner of a DVD-Audio disc will be able to make the copies authorized by the music owner only by using a compliant DVD recorder incorporating the IBM/4C protection approach. When a permitted copy is made, the unique serial number of the blank disc on which the copy is recorded becomes part of the key used to encrypt the content. If a bit-for-bit copy is made onto another blank disc, the serial number of that disc will not allow the proper decryption, and the content won't play.

In developing the scheme, Lotspiech raised the hurdle for would-be hackers, who had already found a loophole in the protection mechanism currently in use on DVD-Video and posted it on the Internet last October. "Because the scheme relied on a single, secret key, once it had been cracked, there was no protection at all," says Lotspiech. His system avoids that danger by relying on so-called broadcast encryption, an offshoot of the scrambling system used by cable TV. Whereas the video protection scheme depends on a single secret key shared by all the discs and the machines that play them, IBM's broadcast encryption scheme assigns a unique set of keys to each player. That is possible because every DVD player contains a bank of 16 "slots," each of which is given a value corresponding to one of 400,000 sites in the key block on the disc (or other medium). The total number of ways of matching the 16 slots with the 400,000 sites is so large — "it's greater than the number of protons in the universe," says Lotspiech, half-joking — that each device can have its own set of slots. Although a particular player may at some point be hacked, and the keys in its slots disseminated over the Internet, those slots can then be invalidated on future media releases. "This invalidation does not hurt the innocent devices," explains Lotspiech, "because they will have at least one slot different from the hacked device."

Ironically, there is one loophole that cryptography cannot block. "Copy protection is only as strong as its weakest link," says Bell. "You can put as much encryption as you want into protecting content on a disc, but for $500 or less you have a cracking device; it's called a DVD player, and out of the back comes a very high-quality analog signal. The notion that analog is inferior is not fundamental; your ears are analog."

That loophole, however, can be circumvented by the use of watermarks — embedded code, unaffected by encryption or decryption, that can also control copy options and that has the added benefit of surviving digital-to-analog conversions. "A compliant device used to copy a disc with a 'single copy allowed' watermark would, in the process, alter the watermark to read 'no more copies.' As a result, any attempt at using a compliant recorder to make a second-generation copy from the authorized copy would fail, even using the analog input," says Bell.

Bell, who has been working with representatives from Matsushita, Toshiba and Intel to make sure that the new scheme's standard corresponds to the requirements of the music industry, acknowledges the challenges that lie ahead. "The distributors have been living in a world of physical stores, and they are now faced with the need to operate in a world of increasingly electronic distribution. It's a difficult and painful transition that will depend on the music companies' willingness to adopt some new business models, but it's going to happen, and a robust copy protection scheme will be critical to its success."

John Lehmann-Haupt is a freelance writer who lives in New York City.