

please keep your TICKET: protecting content and PROPERTY

Things were simpler when I was a kid in northern New Hampshire going to the movies...one ticket, one movie. Not so with multiplex theaters: different shows, different times, and, as I noticed recently, a request that you hold on to your ticket. I wasn't sure why until they asked for my ticket and found I'd paid for Crouching Tiger Hidden Dragon but could have seen *Chocolat*oo.

With movies and other intellectual property quickly moving to various digital forms, it's become increasingly difficult to control access to that property and to assure that its use is paid for properly. The movie theater metaphor isn't perfect, but it does hint at the twin problems of security and rights. Until recently, if you needed to secure intellectual property or files of any sort, you encrypted them. How you did that depended on the state of technology, but it has been an option for centuries. Steganography, "hidden writing," refers to the practice of tattooing a messenger's shaved head. Before delivering the message, he'd let his hair grow back, then—upon reaching the destination—have his head shaved and reveal the message. Strictly speaking, "hidden writing" isn't encryption, although even today it includes clever James Bond-like ways of hiding it.

If I bought a movie ticket back home, I got to see one movie. My "ticket" assured me entrance, analogous to a key allowing me to view content hidden to others who don't have the key. At my neighborhood theater, the owner didn't care if anybody stayed to see the show over and over again. He'd been paid, and didn't have to worry about his (or the movie studio's) rights.

Today, locking content is still important but no longer sufficient. Property rights now include nuances in the way you use the content after you have gained admittance to it. In a recent issue of MIT's *Technology Review*, Digital Rights Management (DRM) was cited as one of the top ten emerging technologies that "will change the world." The reason? Intellectual property is increasingly digital, and Napster has proven how digital delivery provides ample opportunity to circumvent property rights. According to Jupiter Media Metrix, 6% of college book sales in the U.S. will be electronic—not paper—by 2005, compared with one quarter that amount for general consumer book sales. Others estimate \$200-\$300 billion in digital online content. With this much content, combining sound and video, as well as words and graphics gone digital, there is enormous incentive to protect and meter these assets.


Vendors are, of course, rushing to develop products and standards to do just that. Some products involve encryption, but today we've gone from hair to keys, and the longer the key—the tool for disguising digital content—the better the encryption.

Recently, I spoke with Richard Straub, CEO of MediaCrypt, a Zurich-based developer and licensor of encryption algorithm software based on Ascom's International Data Encryption Algorithm (IDEA). This algorithm is built into the

Internet security program PGP, a mail- and file-transfer application. Straub's target is broadband Internet data and digital TV Video-on-Demand, as well as smart cards and Internet banking. Straub expects to have an encryption toolkit for easy and fast integration with such products by mid-2001. MediaCrypt uses a 128-bit block cipher algorithm, considered essentially secure. When I asked about IDEA in set-top boxes preventing pirating of movies, though, he admitted that the "exit point" where the encrypted data becomes unlocked and presented on-screen is "a dangerous point; nobody has a solution yet." What can they provide beyond metering those property rights instead of the binary "view" or "hide" option? Now the techniques get even murkier, and enter Digital Rights Manager, DRM, the "ticket checker".

Looking for rights management solutions gets equally confusing, since many of these vendors are partnering with competitors or cross-licensing their software. Names to watch include InterTrust, Reciprocal, Adobe, Microsoft, and ContentGuard. ContentGuard is aiming to create an industry-standard XML-based digital rights management model called the Extensible Rights Markup Language or "XrML". Content Guard aims to provide a universal method for specifying rights and issuing conditions associated with the use and protection of content, easily integrated into both new and existing systems, from any vendor willing to abide by its free license. You can sign up for information about this standard at <http://www.xrml.org/>, including both the XML model and reference material. XrML has an increasingly large set of followers, including Adobe, HP, barnesandnoble.com, next-generation streaming solution providers like e-Vue, and almost 2,000 other licensees.

When I asked whether IDEA had a digital rights management story, in particular XrML, Straub said he believed XrML would become the standard for DRM. However, Straub's sights are set on "becoming a base technology provider offering an encryption algorithm." When I spoke with Brad Gandee, XrML Standard Evangelist, he too took an arm's-length attitude about encryption: "XrML will work with any encryption standard."

The International Federation of the Phonographic Industry reports that worldwide music sales fell 1.3% in 2000, "the evidence of the impact of free online music." We've gone beyond hair and tattoos to block encipher algorithms and XrML, but selecting the exact solution to protect your content can be like code-busting. The alternative, however, is to take your chances and leave your "theater doors" wide open—something few if any content owners are willing to do. 

Robert J. Boeri (bboeri@ieee.org) is an information architect at a Boston-area financial publishing company.

Comments? Email us at letters@onlineinc.com, or check the masthead for other ways to contact us.