Intellectual-Property Protection Opens Path for E-commerce

George Lawton

One of the hottest areas of e-commerce is the online sale of music, documents, software, and other forms of intellectual property.

To make these efforts successful, however, vendors face a critical concern: how to protect the intellectual property they're trying to sell over the Internet and keep people from copying, forwarding, reselling, or otherwise using it without payment or authorization.

Preventing unauthorized use of intellectual property is a challenge when working in today's online world. Digital technologies enable exact duplication of commercial intellectual property, permitting original-quality reproductions. However, this works for both authorized and unauthorized users. Meanwhile, vendors can use the Internet to sell intellectual property, but individuals can also use it to improperly download and distribute content.

With billions of dollars at stake, vendors are investing in technologies for encrypting intellectual property and defining user rights.

For example, the music industry, which has suffered large-scale piracy with the unauthorized distribution of content provided via MP3 technology, is working on complex standards for protecting their products. (See the sidebar, "Facing the Digital Music.")

Content vendors take different approaches to protecting their intellectual property. Some companies (such as IBM, InterTrust, and Wave Systems) are offering prepackaged multipurpose technologies that vendors of various types of content can purchase.

There are a number of concerns about intellectual-property-protection technology. For example, some people are worried that the technology will give content owners so much control over their material that research scientists, students, journalists, and others will lose the access to intellectual property for academic and public-interest purposes that they have traditionally had.

Nonetheless, the sale of intellectual property has so much potential for generating revenue, vendors plan to aggressively pursue protective technologies.

TRUSTED SYSTEMS

A key concept for intellectual-property-protection technology is the *trusted system*. These systems, which can be devices or applications, can be trusted to follow usage-limitation rules implemented by content owners.

This can be a challenge on the PC platform, though, which is not controlled by content vendors and which makes the copying of content very easy.

"It is difficult on systems that are open," explained Mark Stefik, principal scientist at Xerox PARC, who has conducted extensive research into intellectual-property protection.

This is why much of the work in intellectual-property-protection technology has focused on the PC.

Generally, vendors implement intellectual-property protection by inserting machine-readable tags in the content. The tags, which the content vendor's intellectual-property-protection technology encodes with the applicable usage rights, can be placed into headers or woven into the content file itself. For example, with one music-protection technology, the tags are embedded into

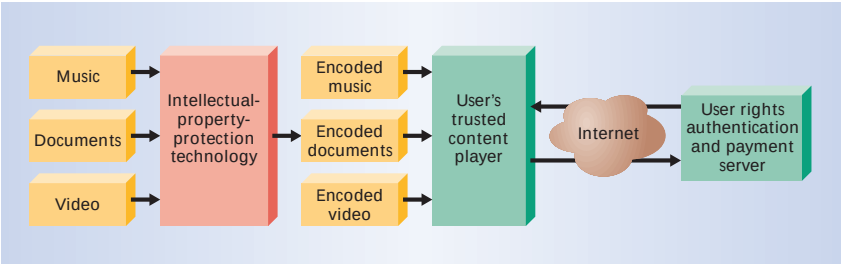

Figure 1. Online content vendors' intellectual-property-protection technology typically encodes music, documents, or video with machine-readable tags. The tags describe how vendors want to limit what users can do with the content, to keep them from playing, copying, or forwarding it without authorization. Trusted content players decode the tags and enforce the limitations, after first verifying with online authentication servers that a user is authorized to access the content.

the file as a subaudible signal.

As shown in Figure 1, a user's trusted device or a trusted application running on a nontrusted device checks with an online authentication and payment server, and verifies that the user has paid for or is otherwise authorized to access the content.The trusted player then decodes the machine-readable tags and plays the content, while enforcing the limitations by the vendor.

For example, machine-readable tags written into plug-in intellectual-property-protection technology from SoftLock. com can instruct players to restrict an individual's ability to copy, save, cut and paste, or otherwise use a specified Adobe Acrobat document in unauthorized ways, said president and CEO Keith Loris.

MULTIPURPOSE APPROACHES

Several vendors have developed multipurpose technologies that content vendors can purchase to protect their intellectual property.

IBM's Cryptolope

IBM has developed a Java-based technology it calls Cryptolope (cryptographic envelope), which can be used to protect audio, video, software, or documents.

Protected content is wrapped in encryption. When a user tries to access the content, either initially or subsequently, the Cryptolope communicates via the Internet with an authentication server. The server verifies the user credentials required to access the product, such as a credit card number for payment or a record of previous payment.

When users properly access the content, a decryption key that is part of software placed on their machine opens the Cryptolope transparently, noted Jeff Lotspiech, research staff member at IBM's Almaden Research Center.

The user's trusted device or application reads any machine-readable tags that are in the content and enforces any usage restrictions, with the help of the Cryptolope opener software, he explained.

The software and the usage restrictions are written in Java, which lets them work across platforms, he said.

Facing the Digital Music

Digital music has become perhaps the most controversial area for intellectual-property protection. The music industry has long-established brick-and-mortar distribution channels but also wants profitable online channels.

However, the widespread unauthorized copying and distribution of digital music threatens both sets of channels. This has led to a flurry of intellectual-property-protection activity.

MP3

One of the key drivers of music sales and piracy on the Internet has been MP3 technology, based on a standard developed by the Motion Picture Experts Group (MPEG). MP3 compresses CD music into files one-twelfth the original size with little quality loss, which makes online music transfer relatively quick.

Content vendors then sell the MP3-based music over the Internet. Buyers can listen to the music over their PC or download it into a Walkman-like MP3 player, made by such companies as Creative Labs, Diamond, and Matsushita/ Panasonic.

i2Go sells this eGo MP3 player.

Forrester Research, a market research firm, projects that the sales of digitally downloaded music could grow from about $1 million in 1999 (compared to $890 million for online CD sales) to $1.1 billion in 2003 (compared to $6.7 billion for online CD sales).

However, there are numerous Web sites that let users download MP3 music for free, without the permission of the content's owners.

SDMI

The Secure Digital Music Initiative consortium of recording industry, consumer electronics, and IT companies has been working on a standard method for protecting MP3 and other types of digital music. SDMI executive director Leonardo Chiariglione said he has never seen such a complex standard progress so rapidly.

SDMI plans to develop the technology in stages. So far, the group has agreed on a subaudible screening signal, called a strong watermark, that will be incorporated into CDs or online music files. The strong watermark is robust enough to maintain its integrity after the music has been compressed with virtually any audio codec, including MP3.

Another data signal, called a weak watermark, will also be embedded in the music. However, this signal will not survive if the music is illegally acquired and compressed for online transmission. Future SDMI-compatible music players would then conclude, if they detect only the strong watermark, that the music was taken from a CD or a music file without authorization and would not play it.

Strong-watermark technology has been developed, but the SDMI consortium is still working on weak-watermark technology. Proponents hope to develop more refined watermark technology that can specify detailed user rights.

A number of vendors have announced plans to support SDMI in future music players, intellectual-property-protection software, and content.

However, Matt Oppenheim, vice president and deputy general counsel of the Recording Industry Artists Association (RIAA), said, "I think there will be no single technology that will stand out as the best technology for all time and all methods of distribution. We will see a quickly evolving variety of technologies, and the best system will be able to adapt as the new technologies are developed."

InterTrust's DigiBox

Like the Cryptolope, InterTrust's technology uses a secure container—the DigiBox—to protect content.

However, with the DigiBox, once users pay for access to protected content, the authentication server, called the InterRights Point, is downloaded onto their machines, explained InterTrust founder and chair David Van Wie. The server then checks occasionally via the Internet with a transaction authority server managed by InterTrust or one of its partners to charge users' accounts, if necessary, and to make sure the accounts are paid in full.

Because the authentication server is on the client, users can access protected content even when offline.

With many systems, when users pay for encrypted intellectual property, they download it and then have to contact an online authentication server to decrypt it each subsequent time they want to access it. This requires them to be online to access the content.

Wave Systems: a hardware approach

Wave Systems has developed a flexible, hardware-based intellectual-property-protection technology, the Embassy chip, which can be embedded in a TV tuner card, a PC, a set-top box, a PDA, or another device.

> Trusted systems are key to enforcing rules that implement intellectual-property protection.

The chip uses an open architecture and is programmable, which lets it host any intellectual-property-protection technology on demand.

A provider would protect its content by developing its product so that it would run only with access to a security applet on the Embassy chip.

Purchasers would then play the content on a device that includes the chip. Each chip offers a unique identifier code so that a piece of content will run only on the machine with the chip.

SOFTWARE: A SPECIAL CASE

A considerable number of software products are sold online. In some ways, software is easy to protect because the developer controls the interface, which limits how users view and work with the product. However, preventing outright piracy of software is a bigger challenge.

Currently, many software vendors control access to their products via a registration-key code. A user must have the code to access the application. Of course, individuals can send the codes to unauthorized users.

Some vendors protect their software by requiring users to attach hardware devices, known as dongles, to PC parallel ports or Macintosh ADB (Apple desktop bus) ports. Application users each have their own unique dongle.

A dongle can be a hardware key or key diskette that an application has to access before running. This adds to the software's cost and thus is generally used only with software that is already expensive or valuable.

Dongles are difficult, but not impossible, to copy. In addition, some crackers have been able to alter dongle-dependent software so it will run without the hardware.

CONCERNS

The use of intellectual-property-protection technology has sparked a number of concerns. One issue is whether the ongoing improvement of technologies that control access to a growing amount of Internet content will make the Web increasingly less open.

However, the most prevalent concerns have been legal and technical.

Legal issues

Some US legal experts are concerned that intellectual-property-protection technology will give owners so much physical control over their content that scholars, researchers, journalists, students, and others will lose their traditional right of fair use.

Under the US doctrine of fair use, an individual can copy and use parts of a copyrighted work in a limited way (such as in a research paper) that does not interfere with the owner's ability to market it.

Some observers are concerned that intellectual-property-protection technology would make it difficult or impossible to access, copy, cut and paste, and otherwise use many documents, photo images, or audio and video clips, even for fair-use purposes.

"I think the issue is whether or not we are going to move to a pay-per-bit world. Copyright law is supposed to be a balance between ensuring a firm's intellectual and financial investment and the need for an educated country that has access to information," said Lesley Ellen Harris, a Washington, D.C., copyright lawyer.

Technical issues

As with other forms of security, vendors realize that crackers could break intellectual-property-protection technology.

Arnold Lutzker, a copyright attorney with Lutzker and Lutzker of Washington, D.C., said much of the Digital Millennium Copyright Act of 1998 applies only to the initial access of content. Therefore, he said, subsequent use of content that was initially accessed without authorization might not violate the law in all cases.

Perhaps the simplest way to break intellectual-property protection is to convert digital music, video, or documents into an analog format and then back to digital, losing the intellectual-property protection in the process. For example, analog music could be played into a PC's sound card, recorded onto the hard drive, and then stored as a digital .wav file.

With documents, a program such as Kleptomania could perform a screen cap

Continued on page 21