On Piracy and Privacy

While a rich set of technologies can be used to combat content piracy, the protection of consumer privacy is dominated by legislative policies and legal agreements.

Savitth Srinivasan
IBM Almaden Research Center

Preventing piracy of copyrighted material and protecting consumer privacy pose major challenges in the digital information age. In a networked digital world, creating, modifying, manipulating, and distributing digital copies of copyrighted content is extremely easy. From a content owner’s perspective, digital content is much harder to manage and control compared to physical assets. Similarly, because advances in telecommunications, storage, and software technologies have made monitoring a person’s activities while surfing the Web effortless, securing personal information and ensuring privacy pose issues of paramount concern to consumers.

Historically, entertainment content owners have responded to the piracy issue by supporting legislative action that prohibits copyright infringement. The information technology industry and service providers constantly seek new business models to support digital distribution of entertainment content.

These emerging business models add yet another dimension of complexity to the piracy and copyright infringement issue, requiring new technologies for content protection and distribution. Recent trends indicate that in the future, content owners may be forced to pursue new distribution models based on consumer preferences. Using the Internet as a distribution channel and computers as rendering devices is appealing because the associated costs and licensing terms are favorable to both producers and consumers.

Somewhat surprisingly, efforts to define, develop, and standardize technologies supporting privacy protection are evolving less rapidly. Privacy protection is often not a core component as enterprises plan and build the architecture of the next generation of digital services. Consequently, current protection schemes for financial institutions, the healthcare industry, and even e-commerce vendors are based predominantly on policy and business or legal agreements rather than on enabling technologies.

PIRACY

Beginning in the early 1990s, concern about piracy of digital goods—in particular, entertainment content—led to the development of digital rights management (DRM) technologies. These technologies dynamically control content throughout its entire life cycle, regulating what can be done with that content and the time frame in which it is accessible. DRM typically encompasses all aspects of content creation, including the definition of associated rights, content distribution and consumption, and the enforcement of authorized rights. It also emphasizes consumer-oriented standard protocols.
and specifications to facilitate interoperability among content owners, service providers, and device manufacturers.

Recent events indicate that the entertainment industry’s position may be softening toward newer content distribution models. Since the late 1990s, the music industry has vigorously battled Internet sites that let users download and copy virtually any song without paying. However, the recent ruling in favor of Morpheus peer-to-peer software, which allows file swapping, appears to be a significant setback to the entertainment industry and is being compared to the landmark decision in 1984 in favor of VCR manufacturers against television content owners.

Apple’s launch of an online music store for Macintosh computer users (www.apple.com/music), which is integrated with iTunes 4, is emerging as a promising alternative to free, pirated music. The service includes more than 200,000 songs from the five major music labels that can be downloaded for 99 cents each with virtually no restrictions on how and where the songs can be played, including on portable devices. Downloaded songs can be played an unlimited number of times and burned to a CD.

Songs are downloaded using the MPEG-2 ISO Advanced Audio Coding standard, which provides higher quality fidelity with smaller file sizes than the older MP3 standard that it extends. Apple uses AAC to tap into the DRM technologies rolled into QuickTime 6.2, preventing users from swapping the tracks as easily as MP3 files. Users can transfer the AAC files they purchase on the iTunes Music Service to another computer, but iTunes 4 and other AAC playback software require the original purchaser’s ID and password to play the downloaded files.

Technology that supports the ability to provide inexpensive, easy-to-access, consumer-friendly models for the purchase and distribution of entertainment content is likely to be adopted, standardized, and widely deployed.

**PRIVACY**

While piracy prevention relies on key technologies, regulations generally mandate consumer privacy protection. The 12th Annual Conference on Computers, Freedom, and Privacy held in April 2002 made it clear that vendors are unlikely to build in privacy protection if there is no incentive for profit, which may account for the current lack of privacy protection applications powered by sophisticated technologies. Protecting consumer privacy thus relies more on policy definition tools and a rules-based authorization engine that enforces access control to sensitive information than on technologies such as encryption, key management, or tamper resistance.

The Platform for Privacy Preferences Project, developed by the World Wide Web Consortium as an emerging industry standard, has been a significant factor in efforts to protect consumer privacy (www.w3.org/P3P) in the face of corporate marketing. P3P provides a simple automated way for users to gain more control over the use of personal information on Web sites they visit.

At its most basic level, P3P is a standardized set of multiple-choice questions, covering all the major aspects of a Web site’s privacy policies. Taken together, the questions present a clear snapshot of how a site handles personal information about its users. P3P-enabled Web sites make this information available in a standard, machine-readable format. P3P-enabled browsers can “read” this snapshot automatically and compare it to the consumer’s own set of privacy preferences.

P3P enhances user control by putting privacy policies where users can find them and in a form they can understand. Most importantly, users can act on what they see.

**IN THIS ISSUE**

In “Protecting Intellectual Property in Digital Multimedia Networks,” Ahmet M. Eskicioglu presents an overview of piracy and privacy issues from a content owner’s perspective, summarizing copyright industry losses due to piracy, the technical means of protecting IP in digital form, and some of the remaining obstacles to secure digital content distribution and storage.

“Protecting Cryptographic Keys: The Trace-and-Revoke Approach” by Dalit Naor and Moni Naor describes two broadcast encryption methods that protect content by creating a legitimate distribution channel. The authors also provide a method for updating user keys to resecure a compromised network and offer a tracing algorithm that uncovers the compromised key’s owner.

In “A Trusted Open Platform,” Paul England and colleagues present an interesting perspective on technologies relevant to an extensible, open computing platform as the basis for a broad class of applications including piracy prevention and privacy protection.

“Preventing Piracy, Reverse Engineering, and Tampering” by Gleb Naumovich and Nasir Memon
focuses on three promising techniques—tamper-proofing, obfuscation, and watermarking—for preserving and protecting software data.

“Technical Challenges of Protecting Digital Entertainment Content” by C. Brendon S. Traw underscores the limitations of currently available technologies in providing a robust piracy prevention solution.

The finance and healthcare industries currently focus on using access control technologies to enforce consumer privacy protection. While some enterprises have adopted the sophisticated P3P policy specification languages, the technologies to enforce these policies are not yet widely deployed. Policies and agreements continue to play a significant role in consumer privacy protection. In contrast, a richer set of technologies including cryptography, key management, tracing traitors, watermarking, and tamper resistance is currently available to prevent content piracy.

If the judgment in favor of Morpheus and Apple’s online music service are indicative of the future, the era of new business models for online distribution of content enabled by a rich set of technologies may finally have arrived.

Savitha Srinivasan is the manager of content management solutions at IBM Almaden Research Center, where she defines new research areas in content management, defines the relevance of copy protection to nonmedia industries, and is actively involved with content-protection standards activities. Her research interests include video segmentation and semantic video retrieval, with a focus on application of speech recognition technologies to multimedia. Srinivasan’s expertise extends into pragmatic aspects of multimedia, including digital rights management. She received an MS in computer science from Pace University. Contact her at savitha@almaden.ibm.com.