Protecting and Managing Electronic Content with a Digital Battery

Timothy A. Budd
Oregon State University

The digital battery's per-use pricing model may be our best hope for protecting artists' livelihoods, generating meaningful usage statistics, and ensuring consumer privacy.

In the days before personal computers became commonplace, a simple and direct system ensured stable relationships between artists, producers, and consumers. An artist would create a work, then give it and certain accompanying rights to a producer. The producer would manufacture a physical artifact that embodied the work, then the producer or its representative would market this artifact, generating a revenue stream—and, incidentally, a measurement of the work's popularity. Finally, the producer would share the resulting revenue with the original artist in direct proportion to the work's popularity—or at least in proportion to a measurable indicator of popularity, such as the number of units sold.

This system of rights, royalties, and limits on reproduction worked for books, records, motion pictures, and other physical media largely because of the difficulty and expense that reproducing them entailed. In the days of vinyl records, for example, few individuals had access to the equipment necessary to produce such recordings. Indeed, only recently have individuals gained widespread access to affordable CD duplicators. Likewise, gallery-quality picture reproductions required sophisticated photographic equipment well outside the reach of most individuals. Reproducing films in celluloid form encountered similar obstacles prior to the development of home videocassette recorders.

Currently, Napster, Gnutella, and other peer-to-peer sharing services have stretched if not broken all these connections, posing such a dire financial threat to content providers that the Recording Industry Association of America and five recording companies have brought suit against Napster.[1] If a consumer can duplicate a digital artifact and share it with a friend, the producer loses any profit from the duplicated artifact and any way to measure the duplicated item's relative popularity. Without a revenue stream or a means for measuring popularity, a producer cannot offer artists appropriate remuneration. Without payment, artists have little incentive for creating new work.

Concerns about generating and measuring revenue have led many to question the long-term viability of the recording, publishing, and video industries. Rampant unauthorized duplication also threatens many other smaller industries that deal in artifacts or ideas amenable to digital representation.[2,3]

0018-9162/01/$10.00 © 2001 IEEE

Fortunately, technology—which helped create this problem—can also provide its solution. To protect intellectual properties, we need a digital system that

- makes unauthorized duplication impossible or at least extremely difficult,
- tracks each use of a given work while ensuring the user's anonymity, and
- can be implemented inexpensively and remain transparent to the consumer.

Such a system would benefit all parties. Producers would receive the revenues due to them, along with valuable marketing information, which would contribute to their financial success and help them continue publishing new content. Artists would receive full royalties for their work, encouraging them to develop additional creative properties. Consumers would enjoy a broader selection of titles, paying only for the content they use, multiplied by how often they use it.

Failure to develop such a system courts a grim future, as the "Commercialism = Creativity" sidebar shows. For, when the financial incentives for creating artworks disappear, art itself withers.

CONTROLLING DIGITAL CONTENT

Today, most home computing systems contain all the technology consumers need to copy MP3 files. Thus, even if the recording companies succeed in reining in Napster, they cannot halt the reproduction of digitized music files in the privacy of users' homes.

Commercialism = Creativity

Always controversial, the management of intellectual property has fostered debates that have only intensified with the advent of legal protections such as patents and copyrights. These measures represent a compromise between that which benefits society as a whole and that which benefits an individual at the expense of the collective. The French Revolution, which took place in the late eighteenth century, provides an instructive example that shows the complex relationship between society, commerce, and intellectual property rights.

Historical precedent

When they first seized power, acting in accordance with their Enlightenment worldview, the revolutionaries abolished all royal privileges, including copyright. Doing so, they felt, advanced society by freeing knowledge from the shackles of commercialism. Heirs to this tradition, today's Napster enthusiasts proclaim with equal fervor that music should be free.

Unfortunately for the French of that time, the absence of copyright and other protections did not cause the products of intellectual thought to flower, but rather to wither. A Paris police commissioner's observation, recorded in 1791, strikes a hauntingly modern note: "There is no author who will consecrate his efforts to the instruction of his century if pirating is made legal." Within a short time, the authorities noted the predictable and catastrophic effects of copyright's abolition—namely, a precipitous decline in the quantity and quality of published works—and restored effective laws.[1]

A persistent legacy

The advent of photocopy centers provides another precursor to our current problems with digital media. Machines that generate paper copies were not widely available until the 1970s. As commercial photocopy centers proliferated during that decade, an increasing number of consumers discovered how they could copy an entire book relatively easily and cheaply —rather than purchase it from the publisher. They proceeded to do so, even though the resulting product usually suffered from inferior paper quality, text reproduction, and binding.

A crisis in the publishing industry seemed imminent,[2] until the US Congress passed new laws and a few high-profile court cases held individuals and copy centers legally responsible for copyright violations. Commercial copy centers became more aggressive in enforcing copyright laws, and in large part the problem of copying entire books dropped to nuisance levels.

Cassette tape recording and videotapes followed a similar path, with minor variations. The producers of videotaped movies managed to create in law a distinction between public and private use. This law permitted duplication of tapes for private use, but forbade the public playback of such videotapes—whether originals or duplicates.

Again, a few high-profile lawsuits cemented this policy in the public mind. The limitation against public use effectively limited the possibility of commercial profit from the production of videotapes to the original producers, thereby reducing the severity of the reproduction problem.

On the other hand, content provider concerns regarding unauthorized copying halted the development of the technology necessary for producing digital cassette tapes for many years. Such concerns remain valid today in locales that have lax or unenforced copyright laws—as is often the case in developing countries.[3]

References

1. C. Hesse, "Enlightenment Epistemology and the Laws of Authorship in Revolutionary France, 1777-1793," *Representations 30*, 1990, pp. 109-137.
2. G. Hardin, "Will Xerox Kill Gutenberg?" *Science*, 2 Dec. 1977, p. 833.
3. R.D. Gopal and G.L. Sanders, "Global Software Piracy: You Can't Get Blood out of a Turnip," *Comm. ACM*, Sept. 2000, pp. 83-89.

The digital battery offers an alternative for tracking and charging for intellectual-property use without alienating users.

Unlike copying and sharing videotapes or books, which require the limited, somewhat difficult, hand-to-hand exchange of a physical artifact, users can infinitely reproduce and instantaneously share MP3 files worldwide with almost no effort.

Given the rapid advances in computing power and storage capacity, the unauthorized reproduction of films, books, and games will soon become as easy as swapping MP3 files. Attempts to control the commercial distribution of digital media thus tend to focus on either limiting reproduction or monitoring use.

Reproduction

Attempts to control reproduction involve technologies that limit the number of times a user can access an item. For example, it is technically possible to create electronic books, so called e-books, that users can read only once. More commonly, developers propose this technique for video sources. Several years ago, a major video rental chain joined with an electronic products retailer to promote a system in which users could purchase inexpensive video disks that they could view only within 48 hours of purchase.[4] The video store reasoned that consumers would adopt this technology as an alternative to rentals because it eliminated the problem of returning a rented video. But consumers failed to embrace the technology, partly because people dislike the idea of paying for a product they cannot freely reuse.

Other recent industry initiatives have also focused on limiting reproduction. Techniques have been proposed that would let a user make a small but limited number of copies of a digital item.[5] Limiting users to one or two copies would let them transfer an item to a repository, but not hand it out to friends. However, given the frequency with which most people reorganize their hard drives—which usually involves the transfer and copy of files—I predict that these technologies will face stiff consumer resistance.

Monitoring

Another proposed approach monitors digital-media use. Some encoding schemes would indelibly brand the content of any digital item—a song, picture, or video.[6] These watermarks would remain with the content as it was reproduced. Display devices would then be modified to recognize this information and transmit an alert to the creator indicating that the consumer is using the item. Some schemes even require authentication before the consumer uses the item: If the consumer has not paid the monthly service charge, the system withholds permission to view the item.

Attempts to determine frequency of use for digital media encounter two major obstacles: portability and anonymity. Such schemes typically involve a combination of

- one-time registration, either via a network connection, post, or telephone, and
- per-use reporting, such as a network connection.

Such a scheme does not work well with truly portable devices like the Sony Walkman, which are not connected to any network. Further, consumers show increasing awareness of the invasive nature of records or databases that maintain information regarding their personal habits. Napster users provided a powerful example of the resistance to this approach when they vehemently objected to EMI's declaration that it would monitor access to Napster files containing works generated by its artists.[6] Consumers expressed these objections even though no one could confirm that EMI had the technology to follow through on its proposal.

THE DIGITAL-BATTERY SOLUTION

The *digital battery* offers an alternative for tracking and charging for intellectual-property use without alienating users, as described in the "Separating Product Distribution and Revenue Generation" sidebar. A metaphor can help us grasp the digital battery's characteristics. While consumers object to content that degrades over time, they do not strongly object when, for example, their portable compact disc player quits working because the batteries die. Yet either event results in loss of access to content. Consumers do not view batteries as being intrinsically tied to particular content. Further, batteries are inexpensive and anonymous.

Key attributes

To be a viable mechanism for monitoring digital media use, a digital battery must have the following attributes:

- *Inexpensive.* A digital battery might cost, for example, $10 and last through several months of typical use.
- *Easy to acquire and use.* There must be no registration. A battery should be available anonymously from a convenient source such as the corner grocery store. Consumers must have absolute confidence that they cannot be linked to a specific digital battery.
- *Limited lifetime.* The two approaches to implementing this attribute resemble a conventional battery: The device can physically deteriorate through use or the system can recharge it in a controlled fashion.
- *Essential to device operation.* Using the digital media presentation device without a digital battery should be impossible.

Separating Product Distribution and Revenue Generation

In the traditional intellectual-property distribution model, shown in Figure A1, an artist creates an artifact that a producer turns into a commercial product. The consumer purchases the product, which generates revenue for the producer. The producer then shares the revenue with the original artist via royalty payments.

The digital-battery model breaks the connection between product distribution and revenue generation, as shown in Figure A2. Artists may still distribute their works through a producer, or they may share their artifacts directly with consumers. The distribution of digital media need not involve any financial transaction: It might, for example, occur over a peer-to-peer sharing network.

In addition to acquiring the digital product, the consumer purchases the digital battery from the battery distributor, which may or may not be the same as the media producer. The battery producer then shares the resulting income with the artist, the producer, or both.

Since deriving royalties only requires registering with the digital battery producer, the digital-battery model lowers the barriers of entry into the commercial marketplace, letting even low-volume artists benefit from this system.

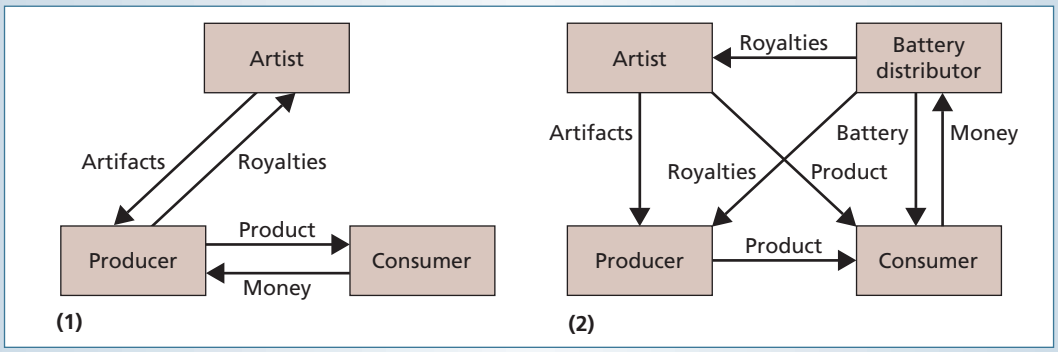

Figure A. (1) The traditional IP distribution model and (2) the digital-battery alternative.

- *Provide use statistics*. The digital battery must include a mechanism that lets the content provider gather statistical information on the use of specific digital-media items, such as how often the device has played a given song.

All these characteristics can be achieved through a combination of cryptology and smart-card technology.

Enabling technologies

Smart cards have been used for many years in devices such as telephone cards and digital-camera media cards. Products of this technology are inexpensive, widely available, and simple to explain and use.

Unlike a credit card, which stores only a limited amount of information on a magnetic stripe, a smart card can incorporate many computational functions.. Further, the card can maintain both transient and permanent nondestructable memory, the latter typically achieved through a process that electronically cuts wires inside the card, much like a fuse. Because they involve an actual physical transformation to the card, these cut wires ensure a limited lifetime, and would-be frauds cannot erase them. On the other hand, to make the card rechargeable, the card maker can encrypt the card's memory to make unauthorized modifications difficult or impossible.

A digital battery would resemble an existing smart card or digital-camera media card. The flat battery would contain contacts that link the card's processor to a larger system, as Figure 1 shows. Card readers would be built into new commercial products or as

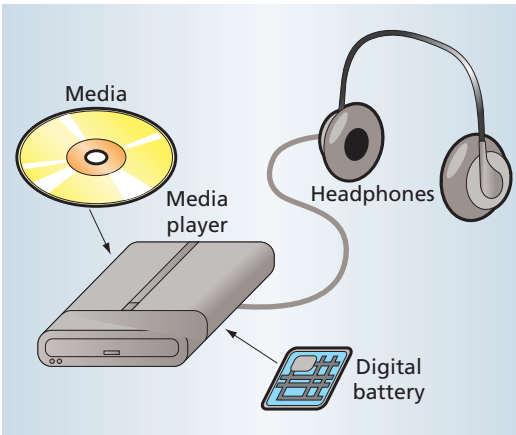

Figure 1. Embedding the digital battery in a media player makes it an unobtrusive component of the system that lets producers charge for content—and compensate artists—on a per-use basis.

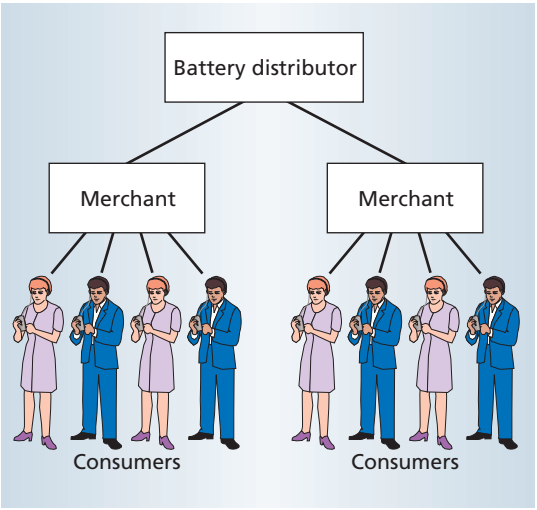

Figure 2. Consumers return used digital batteries to a convenient retail source, such as the corner market. The merchant would amass a large number of returned digital batteries before returning them in bulk to the battery distributor—thereby ensuring individual consumers' privacy while providing accurate usage statistics to content producers.

attachments to existing devices. Using the term digital battery will help convince consumers that the item helps power the digital content presentation and is not the content itself. Thus, distribution of content via networks or Napster-like facilities would be completely independent of the digital battery's distribution and use.

Digital cryptographic techniques can guarantee that transforming digital content into a usable format requires carrying out at least one processing step within the smart card itself. The cards could use well-known algorithms such as RSA or Rijndael[7] for this purpose.

Those familiar with public-key systems might object that this proposal involves using a single key for all media, thus making it a very tempting target for crackers. However, nothing in the basic design prohibits using different keys—and hence different batteries—for different media. Further, an encoding scheme can explicitly permit future modifications to the algorithm.

Admittedly, this approach would require adopting an encoding technique that differs from those currently in use, such as MP3. However, encoding techniques for digital media continue to advance, so this change would not be any more radical than many other media format changes.

A digital battery could monitor the use of all types of digital content, including music, video, print, and images. The battery's software could adjust the rate at which the battery drains to reflect the various costs of different media. A digital battery embedded in a device resembling, say, a videocassette or compact disc player could monitor the use of expensive items such as music or video. A battery connected to a Web browser could record charges amounting to pennies per transaction—so-called micropayments[8]—for accessing Web pages.

BALANCING ANONYMITY AND MEASUREMENT

The digital battery's most innovative feature involves transmitting utilization information back to the content provider. Because the battery itself permanently stores a large amount of information, it can identify the digital content that users access. Embedded software can tie this process to the battery's degradation: When the battery is completely used up, it no longer records information. The task then becomes making the stored information available to the content provider without compromising the user's anonymity.

If the battery uses permanent and unalterable memory, one solution would be for the consumer to pay a deposit for using the digital battery. If a digital battery costs $10, two of those dollars could be the deposit. When the battery's useful life expires, the user could return the battery and retrieve the $2 deposit. This approach provides an incentive, but admittedly no obligation, for the consumer to return the used battery. Most likely, the consumer would return the item to a retail merchant, much like bottle returns, as Figure 2 shows. Because the merchant would aggregate many transactions before forwarding the batteries to the original digital battery or digital content provider, tracing a particular battery to an individual user would be unlikely, if not impossible.

A slightly less secure but perhaps more commercially acceptable technique would let users recharge batteries at a recharging station. For a small fee—less than the battery's original purchase price—a recharging station could read the battery's contents, store the information for transmission to the battery provider, then erase and reset the digital battery for further use. To assure anonymity, the consumer would be exempt from providing any personal information to receive a recharge.

Consumers unconvinced of these policies' effectiveness could simply choose to forgo the deposit or recharging. For the content provider, this approach would reduce the effectiveness of using the digital battery as a means of measuring usage, but it would net profit from the battery itself because the provider doesn't have to refund the deposit. If the content provider is only interested in gross statistical summaries, imprecise usage counts would not be important.

Alternatively, some organizations might elect to collect battery cards much like some groups now collect cans or bottles. Donating a used digital battery to such an organization would eliminate concerns about its data being linked to a particular individual.

After collecting a large number of used digital batteries, or after collecting information from several recharging stations, the content provider could analyze and use the raw data to create statistical summaries that indicate the frequency with which consumers have accessed each digital item. The content provider could, for example, use this information to allocate royalty incomes. Thus, an artist who creates a song that users listen to often will receive a larger share of royalty income from digital-battery sales than an artist who creates a less popular song.

ATTACKS ON DIGITAL BATTERIES

Designed to be a bottleneck between the access and storage of content and its presentation, the digital battery would be an obvious target for fraudulent-use attacks. Avenues of attack would vary, as would possible countermeasures. The most powerful deterrents to circumventing the protection the digital battery provides come from a careful balance between ease of use, complexity of the attack, and economic incentives.

Online attacks

This balance is easiest to see in a situation involving inexpensive content that has a short lifetime—the most frequent target of an *online attack*. During an online attack, the attacker attempts to render the digital battery ineffective in real time as users access and display content.

For example, consider the possibility of a digital battery incorporated into a digital newspaper.[9] Because The cost of any particular newspaper story would be only pennies, or perhaps even fractions of a penny, economic factors by themselves would not drive consumers to seek a means to avoid the expense.

Offline attacks

Continuing with our example, because the newspaper content itself is short-lived, an *offline attack*—in which an individual attacker skirts the protections the battery provides and reposts the material without encryption—would not be economically feasible. Even if such an attack were possible, if consumers can access the contents through legitimate means more easily and quickly than they can access pirated information, they are likely to do the easy thing.

However, the pirating conundrum becomes more problematic when the content is both more expensive and has a longer expected lifetime, such as music or videos. Here, offline attacks pose the greatest danger. To make such an attack, a hacker would need to spend considerable time analyzing and decrypting a single item, in hopes of translating it into a format, such as MP3, which does not require translation by the battery.

Defense against both online and offline attacks must come from several sources. One avenue would be to make decryption so difficult it becomes economically unprofitable. Ironically, the hacker faces the same economic challenge currently facing legitimate industries: ensuring that revenue returns to the creator after the artifact's release.

The courts will, ultimately, provide another form of defense. Concerned parties must aggressively challenge any attempt to profit publicly from the distribution of pirated copies.

Ease of use will form the third leg of the defense framework. Digital-battery providers working with consumer appliance manufacturers must simply make it easier to access digital content legitimately than to pirate it.

Designed to be a bottleneck between the access and storage of content and its presentation, the digital battery would be an obvious target for fraudulent-use attacks.

Achilles' heel

The digital-battery concept suffers a significant weakness in that it uses a single encoding technique to translate all items. For example, the technique could use public-key encryption, but all content items would then use the *same* encryption key. This limitation raises the possibility that a single successful decryption attack on an individual item would forever render ineffectual the protection of all digital content items. While we could make the cost of this process arbitrarily difficult, we could not make it impossible.

One way to solve this problem would be to harness the inexorable progress of Moore's law, which dictates that processing power doubles roughly every 18 months. As more processing power becomes available to the digital battery, new releases could incorporate greater levels of protection while remaining backward-compatible with previous versions. This progression means that newer content items would use more powerful protection schemes, thereby continually raising the bar for would-be hackers. Battery users would only need to upgrade to a new release to get access to the most recent, and best-protected, content.

DIGITAL-BATTERY IMPLICATIONS

The digital battery separates media utilization from media purchase. Most consumers who own a collection of CDs probably have recordings that they purchased, listened to once, then left to gather dust while they enjoy listening to other recordings repeatedly. To the conventional media distributor, both the popular CD and the long-forgotten one represent equally successful sales. Further, once completed, those sales have generated all the revenue that particular distributor would ever receive from them.

The digital battery not only provides more fine-grained information regarding content usage, it continues to provide a revenue stream over the lifetime of the product's utilization. Because income would

amortize over a longer period, the initial investment—the cost of the digital battery itself—would not need to be large.

Obtaining such precise utilization information would accompany—only and paradoxically—a corresponding loss of precision regarding usage patterns for any particular individual. Although we might be able to determine that consumers listen to Britney Spears 10 times more often than to Nine Inch Nails, we cannot determine, except in a broad statistical sense, exactly who listens to Britney Spears and who listens to Nine Inch Nails.

Because their income derives in part from how responsively users—their fans—return used digital batteries, artists would naturally tend to encourage fan participation. Similarly, fans might naturally want to participate by returning used digital batteries to help their favorite content providers, the musicians.

Finally, as with smart cards in Europe, the provider can lease the digital battery's face itself as an advertising revenue source. Providers can encourage users, either directly or indirectly, to collect digital batteries that comprise a limited series, bear images of their favorite stars, or form part of a limited-issue run. Programs such as these will admittedly reduce the likelihood of users returning the battery to the issuer, but because it seeks only large sampling statistics, not exact measurements, the content provider wins either way.

The digital battery's best chance for success stems from its theoretical ease of use, ubiquity, and low cost. As Napster has shown, consumers have few qualms about using pirated artifacts. Nor does guilt over the economic plight of artists appear to create a compelling obstacle to unauthorized copying.

If content providers cannot rely on consumers to do what is morally right, they can nevertheless expect them to do what is easiest, particularly if it doesn't cost them much. If systems that incorporate digital batteries can provide consumers with access to items they desire, and do so in a way that's not overly intrusive, there may yet be hope for rescuing industries that depend on digital content. ✸

References

1. Recording Industries Association of America (RIAA) and Others v. Napster Inc., District Court of Northern California. 10 August 2000.
2. A. Cohen, "A Crisis of Content," *Time*, 2 Oct. 2000.
3. P.J. Huffstutter, "Is a Stitch Online a Crime?," *Los Angles Times*, 1 Aug. 2000.
4. T. Wallack, "No Contest: DVD Prevails in Video Battle," *Boston Herald*, 21 July 1999.
5. SDMI Portable Device Specification, SDMI Secure Digital Music Initiative, July 1999.
6. "If You're Using Napster, You're being watched," CNN.com, 23 Nov. 2000. Available at http://www.cnn.com/2000/TECH/computing/11/24/emusic.is.watching.idg/index.html (current as of 26 June 2001).
7. Rijndael and the Advanced Encryption Standard, http://www.rijndael.com (current as of 26 June 2001).
8. D.C. Denison, "What's a Penny Worth on the Web? Maybe a Lot." *Boston Globe*, 3 Dec., 2000.
9. P. Kunkel, "News Flash: Scrap the Presses—Print and the Web Are Racing Toward the Biggest Media Merger in History," *Wired*, Aug. 2000, pp. 138-148.

***Timothy A. Budd** is an associate professor in the Department of Computer Science, Oregon State University. His research interests include programming languages, object-oriented design, and Web-based education. Budd received a PhD in computer science from Yale University. He is a member of the ACM and an associate member of the IEEE Computer Society. Contact him at budd@cs.orst.edu.*