The Internet Marketplace and Digital Rights Management

Gordon Lyon

***Abstract*—Lacking physical control over Internet receiving environments, traditional information security methods cannot fully protect digital products. Insisting upon physical control severely restricts the Web market for digital objects and stymies e-commerce. Early digital rights management (*DRM*) reflects this dilemma, providing only limited scopes of application and suffering from poor usability. Three views—of customers, of losses, and of applications—help clarify considerations for a less restrictive next-generation *DRM*. Suggestions include expanding the roles of (i) biometrics to ease everyday use and tighten identity binding, and (ii) third parties to substantiate participant credentials and reputations.**

***Index Terms*--Digital products, digital rights management, intellectual property rights, electronic commerce, Internet distribution**

I. Novelties of E-Commerce

Advent of mature Internet services in the 1990s spawned a host of new undertakings, including those in commerce. Electronic commerce (*e-commerce*) is a broad, interdisciplinary field addressing the automation of business through computers and networks. E-commerce gives special emphasis to the public, globally spanning, economical access that the Internet provides.

A. New Mechanisms

E-commerce shows great potential for boosting the efficiency and sweep of current business practices. In addition, e-commerce is an exciting arena that hosts novel forms of transactions, products and services. Business mechanisms that previously were thought awkward or even unrealizable may work well on the Internet. This new power has provided fresh and excellent opportunities for the business imagination. An example can be found in C2C (customer-to-customer) auction markets, which have thrived on innovative mechanisms.

C2C electronic auctions need the Internet's powerful aggregating of participants across dispersed regions and great populations. However, an auction system that runs on computers can do more. Consider a variant of auction bidding that finds a natural home on the Internet. A Vickrey scheme involves each participant submitting a sealed offer [1]. While highest bid establishes the winner, the second highest bid determines the selling price. Because people fixate upon winning an auctioned item more than paying its market value, this split helps dispel "winner's remorse" from overbidding. At least two people are willing to make the second-highest offer, which is what is actually paid. A Web site can automate a close approximation to the Vickrey protocol to support successive rounds of electronic bidding. Used today, the protocol implementation renders electronic auctions quite attractive.

B. New Products and Their Management

The rise of purely digital products has complemented the new mechanisms and opportunities of Web-based commerce. Anyone who has installed new software that immediately "asks" to dial out—automatically—for updates can understand the immediacy and importance of digital products on the Web. These digital fish in the Internet sea may never appear as conventional physical artifacts such as CD-ROMs or paper books. There is no denying digital products are convenient, up-to-date and attractive. However, a widely dispersed Internet market and an elusive, easily duplicated product raise definite business challenges.

Digital Rights Management (*DRM*) is a system of information technology (IT) components and services that strive to distribute and control digital products. Product authenticity, user charges, terms-of-use and expiration of rights are typical concerns of DRM. For a generic DRM transaction, imagine A gets a request to send digital material X to B. The digital content X is typically combined by producer A with tracing information, giving (X + t). This tagged content is then encrypted along with rights-rules (RR) and user/document identifiers (ids) to yield *e(*X +t +RR + ids*)*. A sends this result, *e(...)*, to B. B has a compatible receiving environment, sometimes a special tamper-resistant reader, in which *e(...)* can be properly decrypted and used. The key to *e(...)* may be sent encrypted with B's public key if there is one; B (and only B) then uses its private key to decode the message key. A third-party clearinghouse H receives and sends payments, logs trace information and controls authorizations to A and B as appropriate. See Fig. 1, below.

Early DRM efforts borrowed heavily from computer security technology. However, experience with first generation DRM shows that its context differs significantly from conventional (military style) information security, in which C and D, wishing to communicate information X, *trust*

Manuscript received June 11, 2001. This work was supported in part by the U.S. Department of Commerce, NIST Advanced Technology Program.

G.E. Lyon is with the National Institute of Standards and Technology, Gaithersburg, MD 20899-8951 USA (telephone: 301-975-5679, e-mail: lyon@nist.gov).

each other but worry about unknown agent E learning the content X. In DRM practice, A sends digital material X to B, *but A may neither know nor trust B* [2]. While the encryption and key management technologies of information security are important to DRM, initial DRM methods seem to have overemphasized encryption—the root technology of information security—to the detriment of other vital DRM requirements, such as interoperability and convenience. A balanced, successful next-generation DRM system will have elements that mesh technical, business and legal concerns into a workable, acceptable and open service. One view of this is expressed in [3].

Any obsession with digital product encryption incorporates a certain contradiction and futility. If A does not trust B, then information X is not truly secure when sent. Any number of methods available to B can produce a clear copy of X, free of rules, keys and other DRM control mechanisms. B might send the encrypted *e(...)* to a code-breaking system, tap electronics of a specially modified receiving station at a critical juncture (say within a D/A converter) or even manually transcribe or photograph data from a viewer screen. Should A exert physical control over premises used by B, the picture improves dramatically. Alas, highly controlled receiving environments spoil the business model. E-commerce supposes a large, accessible market deriving from the economy and convenience of open Internet services. In its most richly imagined flowering, e-commerce certainly is not based on controlled, proprietary terminals placed in fixed, physically monitored locations. Accepting open Internet participation means data security is always less than desired, but the volume of business will be considerably higher than would occur with a closed system. This is the dilemma of DRM.

Who might want to steal digital product X? If there is sufficient money to be made, criminals can be counted upon. Political agents are motivated by doctrine, hate and geo-political agendas; they are harder to predict. Governments see geo-political agents as posing the most serious threats. Another group is enthusiasts—*e.g.,* students—for whom the whole process is an intellectually fascinating game. Enthusiasts have a vast talent pool and much available time. Given this cast of several character types, it is worthwhile to look closer at the customer base for digital products.

II. Classifying DRM Customers

Abandoning the idea of full physical control of receiving devices means that customer behavior matters considerably more than it might otherwise. A simple two-dimensional classification of customer behavior helps differentiate and understand cases of risk and potential loss. Dimensions for the customer classification are (i) level of veracity (*honest* or *dishonest*) and (ii) type of interaction (*passive* or *active*). This leads to Table 1 (next page).

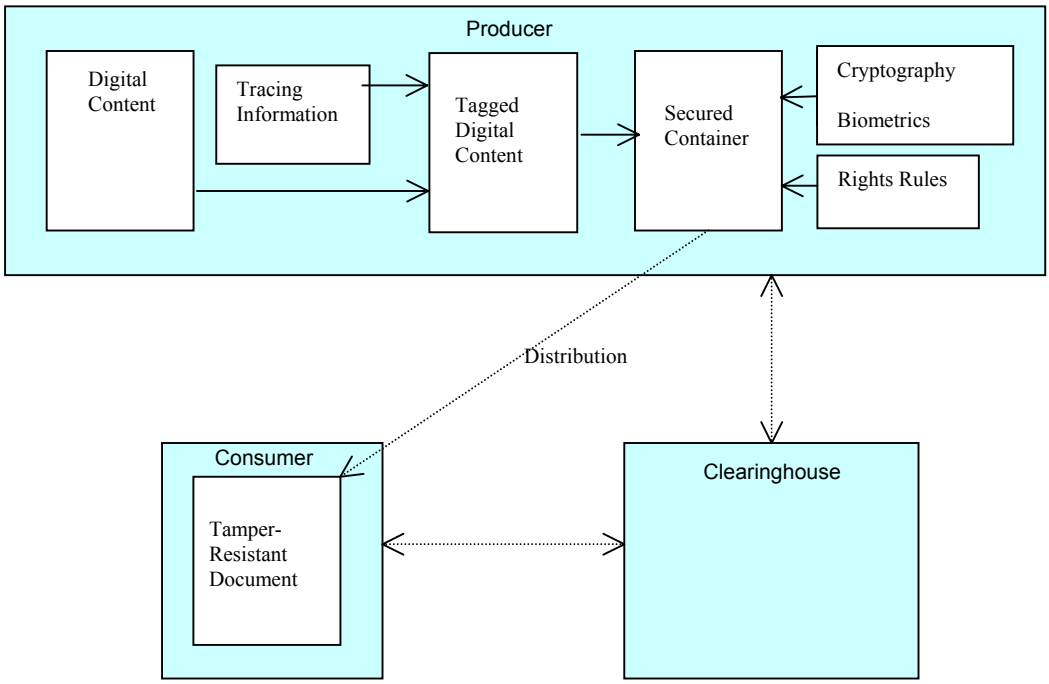

Fig. 1. Stylized DRM flow.

The easiest customer class is that of *honest* and *passive* (denoted *HP*). The HP group obeys agreed-upon rules, makes no effort to find or distribute illegal copies and rejects any stolen materials that may be received. In direct contrast to exemplary behaviors shown by the HPs, the DAs (*dishonest, active*) require constant vigilance. These are the political agents, criminals and unethical enthusiasts identified earlier. It is paramount that infractions of digital rights be interdicted or isolated for this class (subsequent text expands this comment). Central Web servers of stolen materials (typical client-server architecture) must be ruthlessly shut down to make distribution worthwhile. One outstanding problem is P2P distribution—this burgeoning architecture is not well understood at this point [4].

TABLE I
WEB CUSTOMER CHARACTERISTICS

Passive	**HP** (*easiest customers*) --Subscribes without argument --Needs only low information security	**DP** *(mid-level case)* --Prefers per-issue purchase as need arises --Include information security to inhibit swapping
Active	**HA** (*mid-level case*) --DRM maintains fundamental honesty --Infractions are few and inadvertent	**DA** (*worst customers*) --Tough, ruthless cohort --Interdiction of illegal server sites and P2P activity critical
	Honest	Dishonest

Two additional cases fill out the table. These two are more easily handled than case DA, but are not quite as straightforward as HP. An honest and active Web customer (HA) may be a corporate entity (lower left of Table 1). In Western business practice as it has evolved from the Middle Ages, this customer understands the value of reputation and rule of law. Arguments based on invariant legal contexts and good faith participation will have effect. Losses of revenue from these customers are likely inadvertent, generated by the high level of activity within the organization and by its widely known fields of interest. For example, organization members may receive digital materials and use them without realizing that the documents originate from questionable sources. Because HA customers act fundamentally in good faith, DRM is well suited to keeping such participants honest. The HA customers would use DRM to pay for what they use and to check the authenticity of what they receive.

In contrast, dishonest but passive customers, group DP, would like to shake the reins of DRM, but they lack resources to accomplish this. Compliance is grudging: Material is ordered and paid for only as demand arises for it and then, only when it cannot be satisfied by items on hand. Any unauthorized, free versions of materials will be taken opportunistically as encountered. However, such "gifts" are not sought in any diligent, effective manner. The DP customer cannot avoid making valid purchases. The effectiveness of DRM with this group hinges upon successful interdictions in the DA realm to prevent the loss of DP customers. It is useful to look briefly at two cases of product loss.

III. INTERNET AMPLIFICATIONS OF LOSS

A clear (decrypted) version of digital product X, available perhaps via subterfuges discussed earlier, can be duplicated and shipped. Unlike ordinary physical objects, X does not degrade with repeated replication and because of this, warrants examination. Two simple conceptual models illuminate risks posed by unauthorized copying. While arguable on details, the cases illustrate what everyone understands intuitively; copying in some circumstances is benign, but in other instances it is disastrous.

A. Best Case

It is productive to examine two endpoint cases of loss with digital products. In both instances, assume that the maximum Web market is considerably larger than that realized by the product. For example, if there are 400 million potential Web customers, a product will be of interest to perhaps 1-5 million of that number. The best-case model for loss is then trivial. Although decrypted copies of product X are sent to random addresses, the likelihood of an interested customer receiving one is low unless the whole Web address space is blanketed. Customers (type HP) do not actively seek free copies and are willing to subscribe to reliable, controlled e-mailings.

B. Worst Case

In contrast to the above, worst case circumstances demonstrate just how quickly a revenue stream can disappear. Unauthorized duplication does not have to be high for this to happen. In Fig. 2, next page, the upper curve (Replication = 0) plots profits when there is no pirating of example product X. The abscissa represents the number of customers and the ordinate the total profit from sales. Like most products, X is more valued by some customers than by others. Hence, total profit (y-axis) increases ever more slowly with additional customers, the last of whom are very marginal. Eventually product X's per sale profit becomes zero. Authorized distribution of X can cease.

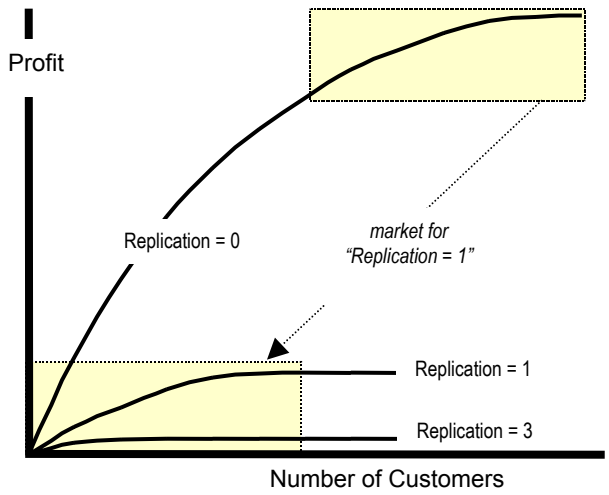

Fig. 2. Worst case amplifications of loss.

Unlike the best case, all worst case customers (type DA) accept, and indeed seek out, free copies in lieu of paying for legitimate deliveries of product X. The most avid customers, who are willing to pay the most, are also the most aggressive in seeking substitute copies of X. Consequently, customers always erode from the most profitable section of any remaining market base. The curves in Figure 1 depict what happens when each authorized copy of X is replicated and distributed once (*Replication = 1* on Figure 1) or three times. Even one replication per authorized copy cuts profits substantially. The problem lies in the pirated copies going to highly interested recipients. Half the customers do pay, but it is unfortunately the half providing the least profitability. The result is a powerful non-linear amplification of loss. *Replication = 3* is a true disaster, with profit near zero. Yet, replication of three copies is trivial; it demands just three "send" commands from the keyboard of each authorized recipient. Think what a Web server offering the unauthorized material could do.

Many different application factors affect risk in digital product distribution. Several of these factors demand attention in initial system planning.

IV. Application Factors

There is no single characterization of the DRM market—risk depends upon an application. Factors such as product design cost, market size and related issues fragment the DRM domain into a large number of segments. Analyses based upon the seven example factors (F1-F7) included here may supply insight as to where DRM works more easily. Notice that this view of an application considers customer type; concern over rule-of-law (F6, below) is an example of the linkage.

F1—Development cost of a digital product.

A more expensive product creates more risk but it also supports a more effective (expensive) tracking mechanism for DRM.

F2—Cost of equipment to use the digital product.

Expensive playback mechanisms limit the market and provide some DRM hooks. If the equipment is specialized enough, it can be controlled indirectly via suppliers. Digital cinema is an example in which the projector alone may cost $120,000-$200,000; storage requirements are also high, requiring at least 45 Gigabytes compressed and 1.3 Terabytes uncompressed.

F3—Number of potential users.

A large market means a product may be difficult to track efficiently, especially if the digital item is quite inexpensive (factor F1).

F4—Digital product reproduction cost.

High costs discourage copying, whereas low costs encourage it. The very size of a digital cinema makes it a more-than-average copying task. An attractive, purely digital product may be marketed deliberately as a clumsier physical artifact—this practice increases reproduction cost and difficulty in the hope of inhibiting piracy [5]. Some equipment can be taxed *upon purchase* against projected copies that likely will be made. CD "burner" equipment and blank CD disks would be examples. The tax is then parceled out by a clearinghouse to digital product publishers according to a formula using popularity and sold copies.

F5—Specific laws apply for a product.

Legislation may assign risks (or rights) that strongly influence a business model. Medical records privacy is an example. Under recent US law, physicians ordering transfers of patient records between medical establishments can be fined for accidental disclosure even though they do not participate in the actual transfers.

F6—Rule-of-law.

DRM contracts need supporting legal contexts that are transparent and predictable. Lack of this support encourages piracy. Problem areas can be isolated from the rest of a product's market. DVD coding regions—six of them world wide—reflect, among other things, a protection strategy. Such a strategy is not necessarily stable, however, for separate regions severely reduce interoperability. Exasperated cosmopolitan users may resort to gray market "extended feature" DVD equipment that handles multiple coding formats.

F7—Product lifetime.

Some material is useful only within a crucial time frame, *e.g.,* morning options-market quotations are not much use later in the day.

Even this simple application framework (factors F1-F7) generates a large number of possibilities, each corresponding to a distinct DRM circumstance. Such variety may be one reason why incidental discussions on digital rights often seem too general. Further examples may help illustrate differences.

A. Digital Cinema

The movie industry would like to replace conventional commercial theater films with computer archives and computer-driven projectors. This promises easier, cheaper and much faster distribution. It would eliminate many quality-control bottlenecks now present in conventional film distribution. A massive, expensive product such as digital cinema should be easier to monitor and track than are MP3 products. For one thing, the high cost of cinema production ($50M—$200M) and its large anticipated profits warrant a more comprehensive (*viz.,* expensive) tracking system. Note that a stolen digital cinema will make no money for a thief unless it can be shown for profit, which definitely generates a public event. There are only about 140,000 cinemas in the world. As mentioned earlier, the projection equipment for public use is very expensive and the suppliers are limited.

B. Digital Format Popular Songs

In contrast to digital cinema, an inexpensively made song recording may prove attractive to millions of private consumers worldwide, each of whom has the equipment to play the digital product with no further expense. It can be hard to track such products efficiently: the product is inexpensive, the market vast. MP3 is a harbinger of these issues. Advent of P2P application architectures renders speculation especially difficult. At present, the area is in an uncertain state; legal issues and technical mechanisms remain unresolved. This makes it hard to design and implement a workable business plan.

C. Special Documents

A specialist's report sells in low volume yet sufficient price (say $50-$5000) that DRM, even a limited, first generation scheme, is useful. The report may come with a custom on-line viewer. To read, the customer may have to request on-the-fly keys from the publisher's central server. Even after a page has been read, saving its old key for a later review will not work, since each page request causes all stored pages to be re-encrypted. Customers tolerate this awkwardness only because they want the results badly.

Imagine an independent auto mechanic reading a manufacturer's service manual for a specific make and model of car. In some countries, e.g., Germany, law requires that such manufacturers' maintenance manuals be made available to independent repair shops. Another example derives from industrial practice. CAD files are now routinely exchanged as proprietary documents among corporations. This may be done without elaborate DRM control; qualified parties are likely all HA types and the materials have limited markets outside of their intended recipients.

V. Discussion

Several topics—customer type, loss amplification, application factors—impact any next-generation of DRM. First-generation DRM emphasis on information security produced poor usability, unpredictable fault recovery and a general lack of interoperability. Given that DRM is an amalgam of technical, legal and business models, then information security techniques (cryptography) are certainly serviceable DRM components, but they are only that. Their protection is never going to be magically absolute, most certainly not in a commercial setting where costs count heavily.

Although not discussed here, tracer information such as watermarks and steganography (hidden watermarks) will aid in establishing digital object provenance for cases of questionable authenticity. Distributors of digital products can monitor their logs carefully to note perturbations that may indicate problems. Practices of distribution must be modified as needed. Risk and the legal element in the overall model must be thought through carefully to keep costs and losses reasonable.

Agreements on distribution should be enforced via civil law, peer/institutional pressure or government actions. In a commercial market, material will leak. A careful business analysis is necessary to understand whether the leakage exceeds what is tolerable within a given setting of customer base, type of loss, and application type. In this context, note that preventive measures to diminish information leakage may be especially efficacious.

The effort to stop distribution of many pirated copies is likely higher than an effort during authorized distribution. One may want to strengthen confidence and trust in the party on the receiving end. A Web-based "vetting" mechanism would qualify recipients of digital materials. As a first measure, individual identity can be tightened through biometrics. This makes it much more difficult for someone to steal or borrow an identity, an issue increasingly pertinent as small wireless appliances deploy. Second, each identity can be substantiated in depth by a third party assurance agent—the clearinghouse of Fig. 1 is one likely host of this service. Combining these two elements, unqualified outsiders should find it significantly harder to get shipments of unauthorized digital material.

A. Strongly Bound Identity

Better identity can be established via biometrics, which provides "automated methods of recognition via physiological or behavioral features" [6]. Biometrics introduces both ease-of-use and stronger binding to the claimed identity. There are no passwords, PINs or pass cards to lose, forget, steal or divulge. A person establishes biometric input values by being present. This biometric identity should be bound to one and only one person, yielding reliable recognition rates and negligible false alarms. Biometrics thus complements DRM security components. For example, with public-private keys, a weakness is protection of private keys. Biometrics strengthens this protection.

The US biometrics industry is currently entering a period of consolidation in which stronger vendors survive and standards become possible. Interoperability and data exchange are evolving, e.g., the Common Biometric Exchange

File Format. Performance and reliability have become important within and among systems. Accuracy is up and prices are falling; face recognition units dropped from $500 in 1999 to $50 in 2001.

Biometrics engineering has reached a level of more mature appreciation. It understands that users do not mind iris scans via ambient light, but—instinctively understanding their own risks—they do object to active retinal scans. American biometrics revenue distributed as follows in 1999: 11% speaker voice verification; 34% finger scan; 3% signature verification; 26% hand geometry; 11% eye scan; 15% face recognition. Increasingly, biometrics combines multi-modal recognition. This helps each contributing biometric method skirt its operational limitations. An instance of a typical weakness is finger scanning. It works acceptably in general, but Asian women may have digit features too fine to register reliably with the current state-of-the-art.

B. Trust and Assurance

A second suggested component in next-generation DRM handles trust and assurance. Even after biometrics has strongly identified an Internet correspondent as *Arun B. of SingaPuraPress*, how much does this tell the distant sender, who does not know this person? The Financial Services Technology Consortium has concluded that lack of trust is a crucial inhibitor of e-commerce [7]. Parties in a DRM distribution need a third party to hold and ascertain credentials vital to digital product distribution: This additional confidential information extends well beyond identity. When *A.Z. of High-Tech Loudspeakers* orders "up to 5000" copies of a software driver for installation in High-Tech's latest run of digital stereo systems, a number of natural questions arise: Is A.Z. authorized to make the purchase? How will a true installation count be established? What are terms of payment? Notice that in answering these questions satisfactorily, trust is being substituted for physical control. Trust can be established remotely. It is thus suited for e-commerce via an open Internet.

First generation DRM systems used a clearinghouse or portal model, which was generally adequate. However, with e-commerce providing a global reach, a more elaborate network of assurance is necessary. FSTC's FAST is a design framework for an inexpensive assurance network [7]. Given parties A and B discussed earlier, A uses a local fiduciary agent F-a, who is linked on *a private trust network* to F-b, a local fiduciary agent for B. Most correspondence between A and B goes over the Internet. Confidential inquires by A about B or B about A travel through their agents over a trusted (and private) link. Payments can also flow through the trust link. The fiduciary agents may provide ratings and recommendations or, for higher fees, they may guarantee their responses and assume elements of risk in the transaction. As inspector or auditor, the agent also re-introduces a (limited) physical presence.

VI. Conclusions

First generation DRM has experienced a commercial context that differs significantly from military-style information security: DRM developments should begin emphasizing elements that mesh technical, business and legal concerns into more acceptable, open Internet services. Several perspectives—of customers, of losses, of applications—help clarify considerations for a less restrictive next-generation DRM. For example, substitutions—discussion mentioned trust in lieu of physical control—may prove useful in designing future DRM frameworks.

Although digital rights management is new, there is growing agreement that usability and interoperability must become principal attributes of a mature DRM infrastructure [8]-[10]. Digital materials should eventually flow to a wide spectrum of users, even if designs are now more limited [11]. Otherwise, burdens of documents in multiple formats and of limited conversion possibilities will dampen market advantages an Internet distribution of digital materials would otherwise enjoy.

Acknowledgment

Thanks to V. McCrary and A. Mink for suggestions on the original text.

References

[1] The Royal Swedish Academy of Sciences Award of the Bank of Sweden Prize in Economic Sciences in Memory of Alfred Nobel, 1996, to Professor James A. Mirrlees, University of Cambridge, U.K. and Professor William Vickrey, Columbia University, New York, USA. http://www.nobel.se/economics/laureates/1996/press.html

[2] C. Potyraj, "Intellectual property rights versus information security," *NSA Tech Trend Notes,* vol. 1, pp. 20-24, Winter 2001.

[3] N. Garnett, "Digital rights management, copyright, and Napster," *SIGecom Exchanges: Newsletter of the ACM Spec. Interest Group on Electronic Commerce*, vol. 2.2, pp. 1-5, http://www.acm.org/sigecom/exchanges.

[4] A. Oram, [Ed.], *Peer-to-Peer*, Sebastopol CA: O'Reilly, 2001.

[5] *Anon*., "DVD-ROM still in contention for digital cinema distribution," DVD Report, vol. 6, pp. 1-2, June 11, 2001.

[6] J.P. Campbell, Jr., L. Alyea, and J. Dunn, "Government applications and operations," *Biometric Consortium Report*, available at http://www.biometrics.org/REPORTS/CTSTG96/.

[7] *FAST Phase I Project Report*, The Financial Services Technology Consortium, 186 pp., Nov. 2000, available at http://www.fstc.org.

[8] J. Duhl, C. Christiansen, and A. Mizoras, "Digital rights management: Fostering trust and privacy for e-business," International Data Corporation white paper, 23 pp., Jan. 2001.

[9] IDRM, a research group of the Internet Research Task Force, http://www.idrm.org, March 2001.

[10] *Anon*., "Digital rights management for e-books: Publisher requirements," Association of American Publishers, Inc., 66 pp., Dec. 2000, available at http://www.publishers.org/home/drm.pdf .

[11] R. Iannella, "Digital rights management (DRM) architectures," *D-Lib Magazine*, vol. 7, circa 15 pp., June 2001, http://www.dlib.org/dlib/june01/iannella/06iannella.html.

G.E. Lyon manages the Distributed Systems Technologies Group of the Convergent Information Systems Division (www.itl.nist.gov/div895) at the National Institute of Standards and Technology (NIST). His group has pursued research in system performance, cluster computing, interactive digital television, and e-commerce. Dr. Lyon began his computing career at the General Motors Research and Development Center, where his first major design responsibility was an experimental typesetting system. He joined NIST in 1972 with a fresh Ph.D. in computer science from The University of Michigan. His numerous technical contributions, which have earned him a Department of Commerce Silver Medal, cover topics such as syntactic pattern recognition, performance measurement, and scatter storage. A recent idea of his, a novel sensitivity-checker for tuning tricky parallel programs, won his NIST team an R&D Magazine RD-100 Award. His professional affiliations include the ACM, IEEE's Computer Society, and the Society for Industrial and Applied Mathematics. He is on the Board of Review for The Journal of Supercomputing, an International Scientific Committee for Institute National des Telecommunications (Evry, France), and the Advisory Council of the Financial Services Technology Consortium.