Commercialization of Electronic Information

JEAN-HENRY MORIN, University of Geneva, Switzerland
DIMITRI KONSTANTAS, University of Geneva, Switzerland

Information dissemination is slowly moving from printed media to electronic media. However this step cannot be completed if the electronic commercialization of information does not provide the same guarantees against copyright infringement as with the printed media. In this paper we present the major requirement for the commercialization of electronic information and describe Hep, an agent-based framework we developed for the commercialization of arbitrary electronic documents over open networks. The Hep electronic document commercialization model follows the secure content encapsulation model and regards documents as programs (agents) that need to be executed in order to reveal their contents. This way the document provider can include arbitrary checks and controls against possible copyright infringement attempts.¹

One of the most valuable commodities in today’s world is information. Business, as well as private persons, purchase every day information provided in different forms, ranging from newspapers to highly specialized business reports, from information video clips to music logos, and from free advertisement to expensive commercial updates. The medium however that dominates the dissemination of information is paper. The majority of information is disseminated in the form of printed documents, from leaflets to magazines and business reports. On the other hand, the vast majority of printed information is prepared using electronic means (i.e., computers). However only a small percentage of the (electronically prepared) commercial information is commercialized in electronic form. For many reasons information providers are very reluctant to commercialize their (valuable) information in electronic form.

Their prudence is well motivated by a number of reasons which become clear if we compare the traditional commercialization of printed documents with the commercialization of their electronic counterparts. With printed documents there are practical limitations to copying, modifying or redistributing a document. For example, it is very expensive, if not impossible, to modify the contents of a printed document without leaving traces, whereas copying a book is in general more expensive than buying a new copy. In addition, even if the printed document is passed from one person to another, there is still a single copy of it. Electronic documents on the other hand can be easily modified, copied, and distributed to many individuals without the original owner losing his own copy and without the need to inform or even get authorization from the publisher of the document. Although techniques exist allowing one to control the integrity of a document and authenticate its publisher in an unambiguous way, the major problem lies in the ability to create and distribute unauthorized copies of the document at virtually no cost. This is eventually the major reason for which commercial intellectual work like books seldom appear in electronic form.

In order to commercialize information in electronic form, a certain number of (basic) requirements, taken from the printed document world to which people are used, should be fulfilled. From the information provider’s point of view, the commercialization of information in electronic form should protect the intellectual rights of the author and/or publisher and guarantee his ability to make profit. On the other hand, the information consumer requires guarantees for...
the authenticity of the information and preservation of his anonymity in accessing it. These requirements combined with marketing needs, like payment policies and trust chains as well as alliances with banking and electronic payment institutions, will greatly influence the design and implementation of any system targeting the commercialization of information in electronic form.

In the last few years a number of systems appeared providing different means for the commercialization of electronic content. The most notable of these systems include IBM’s cryptographic envelopes, Cryptolope (Kaplan, 1996; Kohl, 1997), and InterTrust’s digital box, DigiBox (Sibert, 1995), as well as SoftLock of SoftLock Inc. and Folio4 products of OpenMarket Inc. (Open Market, 1999). The main characteristic of this technology is to bind the usage policy to the content in a secure way. This approach of “boxing up bytes” is commonly known under many terms such as cryptographic content wrappers, boxology or secure content encapsulation. These systems have a strong emphasis on content commercialization, copyright protection and usage metering. However, they have major limitations in that they bind their users to proprietary systems or commercial partners and networks.

In the frame of the Swiss SPI project MEDIA (Konstantas, 1996) we have designed and implemented Hep (Morrin, 1995), a Hypermedia Electronic Publishing agent-based framework for the commercialization of arbitrary information in electronic form and a pilot application, HyperNews, allowing the commercialization of electronic newspapers (Morin, 1997; Morin, 1998). In this paper we present the implementation of Hep and describe the pilot application HyperNews. In the next section we present the concept of Superdistribution and give an overview of the most representative systems in the area of electronic content commercialization. Then we describe the requirements that a system must support for the commercialization of electronic information. Later we present Hep, a framework for the commercialization of electronic documents and some quantitative results of the system. Finally our conclusions and directions are presented.

Superdistribution

The term superdistribution was coined by Ryoichi Mori in 1987 and described in a paper published in 1990 (Mori, 1990). The initial idea was conceived independently by Mori in 1983, as the Software Service System (SSS) (Mori, 1987), and Brad Cox in 1984, as the CopyFree Software (Cox, 1996). Both systems aimed in solving the crucial problem of software distribution enforcing fair compensation to software producers and protection of the software against modification with the least possible burden from the user’s point of view.

Mori observed that while trying to detect whether software was copied (i.e., software piracy) was particularly difficult, it was easier or almost trivial for a program to detect and monitor its use. From there on, he proposes a model where programs are encrypted prior to their release, thus enabling and allowing wide and uncontrolled copying and distribution without any problem of piracy since payment becomes bound to usage rather than to acquisition of the software. Mori describes a set of four desirable properties that must be satisfied for software superdistribution:

- Software products are freely distributed without restriction. The user of a software product pays for using that product, not for possessing it.
- Software products can be executed by any user having the proper equipment, provided that the user adheres to the conditions of use set by the vendor and pays the fees charged by the vendor.
- The proper operation of the superdistribution system, including the enforcement of the conditions set by the vendor, is ensured by tamper-resistant electronic devices such as digitally protected modules.
- The vendor of a software product can set the terms and conditions of its use and the schedule of fees, if any, for its use.

The resulting proposed superdistribution architecture relies on three principal functions: first, administrative arrangements for collecting accounting information on software usage and fees for software usage; second, an accounting process that records and accumulates usage charges, payments and the allocation of usage charges among different software vendors; and last, a defense mechanism utilizing digitally protected modules that protects the system against interference with its proper operation.

In Mori’s design, computers are equipped with a device called Superdistribution Box (S-box). Computers equipped with such devices become S-computers. These boxes are to be understood as tamper-resistant devices embodying microprocessors, RAM, ROM and a real-time clock intended for storage, processing and management of sensitive elements such as deciphering keys and other aspects of the superdistribution system. The resulting encrypted software together with its usage terms and conditions is called an S-program. Its permanent encrypted state has the nice property of enabling it to be transmitted over untrusted and insecure communication channels. Furthermore, since programs are encrypted, they can be copied and distributed by anybody without causing any prejudice.

In doing so, Mori turns a major drawback into a major asset. Namely, the inherent nature of software that allows it to be copied and distributed in a marginal, cost-effective way, turns out to be a real asset. In this scope, users become themselves “legal” re-distributors of software they like and use most. Based on this work, two prototype S-box systems were built: the first one based on a NEC9801 personal computer in 1987; the second built as a co-processor for a Macintosh in 1990.