Secure Multimedia Content Delivery to the Home via the Internet

Matthew Barrett
CompSci.725, University of Auckland
mbar116@ec.auckland.ac.nz

1 Abstract

The unauthorised distribution of multimedia content over the Internet is a growing problem. The ease of digital duplication and the failure of previous technical solutions to overcome the leakage problem have driven the development of end-to-end content delivery solutions. The technical implementation of two such systems, CPRM and ODCP, are discussed. A detailed description of the entities involved, and an overview of the processes with which they operate is given. Some limitations and weaknesses are given, and improvements to ODCP are suggested. A modified ODCP architecture is described, derived from systems given in other literature.

2 Introduction

The illegal distribution of music and movies via the Internet has resulted in numerous attempts by the industries affected to implement technical measures to curtail it. Such technical implementations are both interesting and concerning from a software security point of view. The implementation of these techniques borrows from the fields of cryptography, watermarking, digital authentication and many others. If implemented to the extent that the effected industries would like, there may be a restriction in, firstly, well established fair use rights in the United States of America, and secondly, in the ability of a consumer to use his personal computer as he wants.

Two schemes that have been proposed to curtail the piracy problem are CPRM and ODCP. A discussion of the implementations of these is instructive. Furthermore, weaknesses in ODCP can be reduced, and the feature set as a whole improved, by modifications derived from literature describing the prevention of unauthorised execution of software. An attempt is made to develop a more secure scheme that results in fewer reductions to existing usages of personal computers, whilst still allowing delivery via the Internet to the home.

2.1 Digital Duplication

CDs and DVDs are now the preferred method of large-scale distribution of audio and video to home users. Their increased convenience, quality and cost-effectiveness have ensured their rapid and widespread uptake in developed countries the world over. Such digital media allows flawless

reproduction, time and time again. There remains a limitation to this method of distribution – duplication requires a physical copy to be available.

Copies of CDs made from original, or duplicate physical media can spread between friends and associates in a fairly limited geographical area. The Internet allows for the transfer of a compressed music track across the globe in minutes. The degradation in quality by compression is, too many users, indistinguishable or outweighed by the convenience and cost that the download brings over traditional and legitimate means of acquiring music.

Currently, the distribution of movies has yet to gain the critical mass of that music. However, rapid advances of compression technology in the last few years has seen acceptable quality facsimiles decrease in size to that of a CD – around 700MBs. With the increased uptake of broadband for home users, such files can be easily downloaded over night. There is little doubt that as compression technology improves, and as bandwidth both cheapens in price and increases in availability to the home user, more movies will be illegally distributed via the Internet, most commonly through peer-to-peer networks.

There is an obvious need for a method of distribution which takes advantage of the low cost and ease of the Internet, yet ensures that copyright holders are compensated for use of their products.

3 Solutions

From a discussion of the piracy problem, it is obvious that copyright holders feel the need to protect their assets. A number of solutions have been implemented, with varying success.

3.1 Technical

The current state of technology provides inadequate controls to limit unauthorised distribution of content. Currently, there are a few solutions available. Digital Versatile Disc (DVD) technology was protected, when first released, with the Content Scrambling System (CSS). In November of 1999, in an event that has received widespread publicity since, DeCSS was released. This system allowed the decryption and subsequent unencrypted storage of the encrypted data stored on the DVD. Despite the system being initially broken as a result of sloppiness on the part of a software company, weaknesses in the encryption algorithm allowed the generation of other keys. In response, the DVD CCA (Content Control Association) sued over 500 individuals.

3.2 Leakage

The failure of CSS illustrates the leakage problem. Solving the aforementioned piracy problems with cryptographic tools originally designed to provide privacy between end users through symmetric or

asymmetric encryption results in a mismatch between the problem and the solution. Strong encryption has limited feasibility when you consider the processing requirements for gigabytes of data, and the limited processing power available in set top boxes. Content must be decrypted at some point to be presented in its final form to the consumer. The security and continued success of any scheme based on encryption depends on the secrecy of keys. As DeCSS has shown, it has so far been impossible to ensure that no copies of the secret key will become available. If they do, they can be distributed far and wide. Any content encrypted with it becomes immediately available. Once decrypted, there is no ability to limit the distribution of the material, nor its modification into other forms (compression). This is known as leakage. Any scheme which relies on encryption to prevent copying and distribution relies on the encryption remaining intact, and the decryption keys remaining a secret.

3.3 Digital Watermarks

In response to the leakage problem, researchers developed digital watermarking schemes. Yu in [1] gives a instructive description of digital watermarking. It is useful for copy protection schemes because it allows the embedding of a secondary data stream into the media stream of audio or video content. This data stream can contain authentication information or usage restrictions. Two forms of watermarking exist – robust and fragile. A robust watermark is intended to resist decompression and recompression of a data stream, as well as to have some level of resistance to malicious attacks. A fragile watermark is one that has none of these properties, and relies on the data stream to remain unmodified. Watermarking has its limitations however. It relies on the modification of data in a content data stream in such a way that the resultant stream is not perceptively different. The most popular and efficient audio and video compression schemes, however, rely on the removal of such imperceptible information from the data stream.

3.4 Added Value

Karp in [2] states that the technical and legal systems being implemented by the motion picture and recording industry associations are not required. He gives an example of the pornography industry, whose products can be copied easily, and without restriction.

Karp states that the pornography industry adds enough added-value to their product, through the use of high quality web sites and other meta-information, that paying for the content is made worthwhile. He suggests that the traditional recording and motion picture industries may find it easier to combat piracy by making sure that the services received through purchasing music legitimately are of a high enough value to warrant the associated monetary cost to the consumer.

3.5 Legal

Traw et al in [3] state that technical means of preventing unauthorised copying and distribution work best for unsophisticated attempts to circumvent them by home users, and individuals in general. Schneier in [4] agrees. Traw goes on to state that at the other end of the scale, legal systems work best for protecting content from unauthorised use by businesses. An in depth analysis of all the legal means that are available to protect copyrighted material is outside the scope of this paper. However the advent of the DMCA, in the United States of America, makes the research, creation and distribution of programs designed to circumvent the technical systems protecting copyrighted work illegal [5].

4 End-To-End Solutions

From the description of the piracy problem given, and an understanding of the leakage problem and the limitations of current technical schemes, it has been concluded that to fully secure multimedia content, an end-to-end solution is required. An end-to-end solution is one in which the content is encrypted throughout the entire delivery chain, all the way up until it is consumed by viewing or listening on a device. Whilst the media can always be recovered in an analogue format when played back, the aim of an end-to-end solution is to prevent digital copies of the content being acquired in an unencrypted form.

4.1 Two Proposed Solutions

Two proposals, both aiming to provide an end-to-end solution for multimedia content, are the CPRM (Content Protection for Recordable Media) proposal, described in [3] by Brendan and Traw, and the ODCP (On Demand Content Protection) scheme described by Zhang et al in [6].

4.1.1 Descriptions

CPRM is a proprietary technology developed by the 4C Entity, a combined grouping of the following companies: Intel, IBM, Toshiba and Matsushita (Panasonic). It was developed primarily for use in removable media, but has been proposed for addition into the ATA specification for hard disks. The proposal met with harsh criticism, and was not implemented. It is instructive to review the proposal, how it works to prevent unauthorised viewing of multimedia content, and the ramifications that would come about should it ever be implemented.

ODCP is a proposal presented by Zhang et al in their paper [6]. It has no commercial backers, and is described in a conceptual manner. It is intended to allow for secure media-on-demand delivery to authenticated users over the Internet. It also has a number of similarities with the system architecture

proposed in [7] by Maña and Pimentel

4.1.2 Goals

The goal of CPRM is to prevent the unauthorised viewing and copying of digital content. It aims to solve the leakage problem previously described by working with other technical specifications from the 4C Entity to provide an end-to-end solution. CPRM is the most relevant of the related technologies for this discussion, as it allows for the distribution of content over the Internet. I will describe in detail how CPRM aims to solve the leakage problem when discussing its technical implementation.

ODCP aims to prevent the unauthorised viewing of multimedia content. The authors describe its usage in a Media on Demand (MOD) network, to provide an end-to-end solution for the delivery and consumption of multimedia. The authors aim to solve the leakage problem by restricting the devices which are able to play back the media stream.

4.2 Technical Implementations & Operation - CPRM

Despite claims by the 4C Entity that the CPRM specification had been made available, I was unable to find any published, peer-reviewed articles other than that by Traw et al [3]. Their paper provides a technical description of some of the components of CPRM; the C2 cipher, and the media key blocks. They also give a description of its operation. Schneier in [4] provides a much more informative description of the system architecture as a whole. I will explain CPRM by first describing its various entities in detail. An in depth discussion of the technical operation of CPRM would require more space than what is available for this paper, however some detail will be given with regards to its unique technical features. I will describe the possible processes through which it could operate. Finally, I will describe some possible limitations and criticisms of the scheme.

4.2.1 Entities

The CPRM system has three main entities:

CPRM compliant media that differs from normal media in that it contains a Media Key Block (MKB), and a unique media identifier.

CPRM compliant disk drives that differ from normal media by having an extended ATA interface through which CPRM calls are made. They also contain a unique combination of 16 secret device keys.

CPRM compliant software that communicates directly with the compliant disk drive, bypassing standard operating system calls.

The MKB that exists on CPRM compliant media is a table of cryptographic information used in the

decryption and encryption process. The table can be logically represented as a two-dimensional array, with 16 columns. The unique media identifier is located in a region of the media that consumer-level DVD authoring equipment is unable to modify. All CPRM compliant devices are able to store and manipulate files that are not encrypted with the CPRM scheme, and operate as a normal entity would.

A CPRM compliant disk drive is required to use CPRM compliant media. A compliant disk drive will be given 16 unique and secret device keys. Each of the 16 keys is chosen from a row in a different column of the MKB. The combination of keys is unique to each device, and can be used to uniquely identify a specific device.

CPRM compliant software is required to access the CPRM features of devices and media. According to Schneier [4], CPRM compliant software will encrypt the file based on the unique media identifier found on compliant media, which can be read by a compliant drive.

The encryption and decryption of files in the CPRM scheme is handled by the C2 cipher. The C2 cipher was developed for specific use in the CPRM scheme because, according to Traw [3], there are no other schemes available which meet the required functionality and are easily applicable to both hardware and software implementation, without excessive licensing. By creating a cipher for use exclusively in CPRM, the 4C Entity has ensured that they can license the technology to interested parties. Traw also states a benefit of using an exclusive cipher means that any circumvention of the scheme by third parties will infringe upon 4C Entity patents. Any attempt to circumvent the system is also an offence under the DMCA in the United States of America.

4.2.2 Processes

The C2 cipher is a 10-round block cipher with a 64-bit block size and a 56-bit key [3]. It's specific operation and implementation is outside the scope of this discussion. However, a discussion of the operation of CPRM will illustrate some of the C2 cipher's features.

CPRM has two operations that are of relevance to secure content delivery over the Internet. The first is when media is initially stored on to a user's personal computer. The second is when a copy is made, to either other CPRM compliant media, or to a normal disk. Schneier [4] gives an instructive description of the proposed operation of the delivery of media over the Internet to the user's personal computer. Combining this with information provided by Traw [3] a complete picture of CPRM's operation can be arrived at.

A user will request content through a CPRM compliant application. Content will be delivered to the compliant application through a secure process external to CPRM itself. Once the content is on the user's personal computer, it is encrypted by the compliant software and a compliant device. This

process will use the unique media identification read through a CPRM compliant drive, along with another number (an increment-only counter) retrieved from the media. This number, unlike the unique identifier, can be modified. But as part of the CPRM specification, compliant devices will only allow this counter to be incremented, never decrement or set to a specific value. These two pieces of data are hashed with a one-way hash function of C2. The output of this hash function is used to encrypt a randomly generated 'title key' with the C2 cipher encryption function. This encrypted key is then written as an ordinary file to the media. The title key and the content's CCI (Copy Control Information – access rights and usage limitations that are upheld by CPRM compliant devices) are fed into the C2 cipher's one way hash function. The output of this function is, finally, used as the key to encrypt the content itself, using the C2 cipher's cipher-block chaining mode. This process ties the encrypted content to the media on which it resides; it cannot be read unless decrypted with the proprietary C2 cipher, which allows the CPRM compliant devices and software to enforce the CCI restrictions.

The other process in which CPRM operates is when a user attempts to copy or move the protected file. The implementation of CPRM allows any file copied to another medium to be considered logically 'moved,' not duplicated as in a normal copy. Access to the initial copy of the file is revoked, and CPRM implements a set of safeguards to ensure that access to the file is cryptographically impossible.

An extremely important feature of the CPRM system, mentioned by Traw [3] but not by Schneier[4], is the use of a watermarking scheme. As previously mentioned, unprotected files are able to be stored on CPRM media. However, as part of the CPRM specification, when they are played back they must be checked for the presence of a watermark. This watermark may contain CCI data that may cause the device to block access to the file.

4.2.3 Limitations

As the processes described illustrate, the leakage problem is addressed in CPRM by attempting to restrict what entities are able to access the unencrypted file. Schneier in [4] critiques the scheme, claiming it will be ineffective. He argues this by stating that any copy-protection scheme that has a basis in software will fail. This is also the conclusion reached by Maña et al in [7] who develop their scheme based on the premise that to obtain a provable secure protection scheme, execution of the software must be based in hardware. Schneier believes that it is only a matter of time before a method to obtain the decrypted content from the CPRM compliant software, immediately before it is played back, becomes available.

The 4C Entity's ideal implementation of CPRM, however, includes a complete end-to-end solution, in which decryption takes place in the device, such as a TV or stereo, which plays the content. Content is transferred to these devices through other protocols and specifications developed by the 4C Entity. If the content protected by CPRM were to include a robust digital watermarking scheme, as previously described, then the scheme would grow in strength considerably. If CPRM compliant hardware becomes widespread, the play back of decrypted files that were originally CPRM encrypted would become difficult, and reliant on the ownership of hardware devices that were not CPRM compliant. The scheme would become limited by the quality and robustness of the watermarking scheme employed.

The ramifications of this scheme, should it ever achieve wide-spread implementation, would have huge collateral effects on the use of personal computers by consumers

4.3 Technical Implementations & Operation - ODCP

I will describe ODCP in a similar manner to CPRM. First, I will describe the various entities of ODCP. Because the authors do not give any technical implementation details of interest, I will then discuss the processes by which ODCP is intended to operate. Finally, I will discuss some weaknesses of the scheme, and give some possible improvements.

4.3.1 Entities

The ODCP system has three main entities:

The MOD (Media On Demand) server. This is the server that handles requests from users for content and delivers the content back to the user. This is under the administration of the service provider.

The SMS (Subscriber Management System) server. This is the server that handles user authentication, and user entitlement requests, and is also under the administration of the service provider.

Media players. These are devices owned by the user that are able to playback media delivered through the system They can be either personal computers, set-top boxes, or portable music players. These devices can be manufactured by third parties, and simply adhere to a published standard for ODCP operation.

4.3.2 Processes

All media served to users via the MOD server is encrypted with a 'content key.' Each item of content available on the MOD server should be encrypted with a unique content key, and these keys should be stored in a secure location. Content should be encrypted the first time it is made available to users on the MOD server. The authors do not propose a specific encryption scheme for ODCP, but state that the encryption used should depend on the sensitivity or type of data being encrypted.

An important feature of the ODCP scheme is that once encrypted, content can be made freely available and distributed through any number of channels. Users can make copies of any media they have previously received from the MOD server, and distribute it to their friends or associates. Users are able to receive media through peer-to-peer networks, for example. All content should be uniquely identified, both on the MOD server and when distributed through various other channels. The authors give no indication of how this should be done.

To be able to play back any media that the user has obtained, the user must obtain the content key with which the content was encrypted. To do this, the user must first have an account of some sort with the SMS server. When creating the account for the user, the SMS server generates a set of secret keys. No mention is made by the authors as to whether these keys should facilitate symmetric or asymmetric encryption, but it appears that they intend to use symmetric key encryption. I will show in a later section how we can use Maña et al's asymmetric scheme to improve the ODCP architecture and security. This newly generated key set is kept secret from the user at all times, but the user is given a unique user ID with which to identify himself to the system in the future.

The next phase in obtaining the content keys for desired media play back is for the user to register those devices on which he wishes to play back the media. The authors describe two ways in which this can be accomplished. One is done purely in software, and can be performed over the Internet. The other requires the service provider to send the user a smart card. The intent of registration is for the players to obtain the secret keys of the user. The software process described by the authors is poorly developed, and inherently weak. It will not be discussed here, but possible improvements on the user of hardware registration will be discussed in a later section.

The hardware process requires the use of smart cards, and is intended to be used with set-top boxes, or portable music devices which would both incorporate smart card readers. The service provider, after the subscription process has generated the user's set of secret keys, sends the user a smart card containing the user's secret key and user ID. With this smart card, a user can register any number of players that are equipped with smart card readers by simply inserting the smart card into the device. The authors do not state if the secret key should be stored in the player, or obtained from the smart card each time it is required.

These two steps, user subscription and player registration, must occur in the order described here, before the user can obtain an 'entitlement' to play any media. To obtain an entitlement, which contains the unique content key to allow decryption of the content the user wishes to play back, the user submits a request to the SMS server. The request includes the unique ID of the content the user

wishes to play, along with a user ID and password. The reply, encrypted with the secret key of the user, contains the content key, related information required for decryption, and a usage rule. The usage rule allows the service provider or copyright holder to specify how and when content can be played back. Once an entitlement has been obtained, a process which requires a connection to the SMS server over the Internet, it can be distributed to all other registered players. Since they have already obtained a copy of the user's key set, they are able to decrypt the entitlement message, obtain the content key, and decrypt and play back the desired content at any point in time. This allows devices to play back the media where or when a network connection is unavailable, either through failure, or in the case of portable devices, not physically present.

4.3.3 Weaknesses

As mentioned in the discussion of ODCP, there are a number of significant areas of weakness in the presentation of ODCP in [6]. The authors description fails to clearly state what forms of encryption should be used in the various parts of the system. By allowing software registration to occur, the authors introduce a crucial area for possible attacks to occur, and weaken the entire scheme considerably. By using a unique identification generated from the user's hardware, the authors open up another possible avenue of attack, by fabrication or modification of the hardware signatures used to create this ID. Finally, the distribution methods used for the user's secret keys are relatively insecure.

5 Improvements

In [7] Maña and Pimentel describe a scheme to prevent the unauthorised execution of software. A number of the features of their scheme can be developed to improve the overall security of ODCP. With some modifications, Maña and Pimentel's software protection scheme can be used to protect content from unauthorised viewing. The paper describing Maña et al's scheme provides more detail than is required here. A working knowledge of it is assumed by the reader. The implementations described in [7] will be discussed only in as far as they can be modified and applied to ODCP. I will present the modifications in four parts – as they relate to the issues raised above, and a fifth section in which changes to the general architecture will be discussed.

5.1 Encryption Methods

Maña et al describe the usage of symmetric encryption to encrypt software. The use of symmetric encryption provides improvements in speed and efficiency over the use of asymmetric encryption when used to encrypt content. Given the low processing and memory specifications of the set-top boxes and portable music players intended for use with ODCP, such improvements are crucial.

Content should be encrypted with a unique symmetric key when made available for users as in the original ODCP system.

5.2 Software Registration

A modified ODCP scheme would not have any form of software registration. Instead, if a personal computer was desired to be able to play back multimedia content, it would require a smart card reader. The low cost of such devices would not make the scheme unfeasible. Consumers would already be comfortable with the idea of using smart cards from their use with set top boxes. A service provider that provides a set top box to a subscriber would also provide a smart card reader as a complimentary or premium service.

By allowing the use of a personal computer to consume content, a weakness is introduced to the scheme. The ability to use a personal computer to bring multimedia content securely into the home via the Internet is considered highly desirable. However, compromises must be made if the personal computer is to be allowed to consume the content itself.

5.3 Unique Identification

A unique identifier generated from the user's hardware is used in the original ODCP scheme to encrypt the entitlement message specifically for that user. In the modified scheme, the user's smart card, obtained during the subscription process, contains the uniquely identifying information. It should be in the form of an asymmetric key pair, the public key of which can be kept by service provider to aid in authentication of digitally signed messages from the user.

5.4 Distribution of Secrets

One of the critical weaknesses in the original ODCP scheme is the insecure way in which secrets are distributed to users to enable decryption of content. Maña et al describe in [7] a very powerful license generation and management scheme. In order for such a scheme to be implemented with ODCP, only minor changes are required. A user is still able to obtain the content through various distribution channels. In order to obtain the symmetric key with which the content is encrypted, the user sends a digitally signed message authenticating himself to the SMS server as in the original scheme. The SMS server replies with a message containing the symmetric key used to encrypt the content the user wishes to view encrypted with the user's public key. The decryption of this message can only occur with the user's private key, which is stored securely on the smart card (As in Maña's scheme, tamper-proof smart cards are required).

The user's smart card will now contain an entitlement for the user to view that content. The smart card can be inserted into any compatible device to enable playback of the content, any where and at

any time. A network connection is not required for authentication, as in the original ODCP scheme.

5.5 General Architecture

The use of Maña et al's scheme to prevent the unauthorised execution of software requires that encrypted code be decrypted and executed on the smart card, with only the unencrypted results being returned. When using the scheme to protect content this method of operation is not possible as the unencrypted content must be made available for consumption at some point. The decryption process will also require resources such as processing speed and memory that are not available inside the smart card. When content is to be consumed on a set-top box, portable music device or some other black-box like consumer electronics device, the symmetric key used to decrypt the content can be transmitted outside the smart card, and be used by the device itself to decrypt the content. Encrypting the symmetric key again, before this transmission takes place, with an asymmetric key pair generated for the device, can increase the difficulty of obtaining a clear-text copy of the content decryption keys.

A smart card reader/writer is required for the acquisition of licences to play content. This entitlement process must take place on a personal computer attached to the Internet, or via an interface provided through a set top box communicating with the SMS server via a phone line. In order to ensure that content is securely managed on a personal computer, which has the ability to be modified and inspected to a far higher degree than a normal consumer electronics device, it may prove impossible to implement the scheme without some of the significant changes in hardware required by a scheme such as CPRM. It may be necessary to forgo the ability to play back the content on a personal computer, as once decrypted, it is generally understood that eventually a method of obtaining the decrypted content will be found, and leakage will occur.

6 Conclusions

From an overview of current and past technical systems used to attempt to stop the unauthorised distribution and viewing of multimedia content, it can be seen that new technology and implementations are required. The failure of CSS to protect DVD video content is an illustration of the difficulty in ensuring the leakage of content does not occur. The use of digital watermarking shows promise by allowing data to be embedding into a content stream in a manner which is difficult to remove. In order for digital watermarking to succeed as a method of controlling distribution and playback, however, new devices which check for and enforce the data found in the content stream must be in widespread use.

CPRM is one such system which can be used to enforce both digital watermarks and restrictions on

copying and viewing of content. CPRM is failing to gain acceptance however, because of the draconian limitations it places on general and existing usage of a personal computer.

The use of a system such as ODCP, which does not require the modification of hardware, software or media that CPRM does is more likely to gain acceptance, and will be seen as less of an intrusion into people's rights and privacy.

The ramifications of a system to allow secure content delivery to the home must be weighed against, in the US, existing fair use rights. Numerous authors in the field of software security have raised concerns about the encroachment on privacy, and the removal of legitimate fair use rights that DRM schemes can bring.

It is concluded after an examination of the proposed ODCP scheme, that a number of improvements can be made. Ideas and implementations taken from Maña et al's scheme designed to prevent the unauthorised execution of software can be applied to create a more secure, more robust version of ODCP. More work can be done in this area, in order to obtain a full specification from which a working implementation could be derived. However, I hope to have shown the improvements and success such a system would have.

I feel that it is reasonable to conclude that in order for secure multimedia content delivery to the home to gain widespread acceptance with consumers, a mindset change must occur. Consumers are currently used to the physical purchase of a CD or DVD of which they retain ownership at all times. A shift to the digital distribution of content must be carefully managed to ensure success. It may be possible to use a personal computer to obtain content, and entitlements to view that content. The actual play back may be performed on a separate device elsewhere in the home. This is one possible way in which the benefits of an Internet distribution channel can be utilised by media companies who still wish to receive profits for their copyrighted materials.

7 References

[2] Karp, Alan H. "Making Money Selling Content That Others Are Giving Away." Communications of the ACM 46, no. 1 (2003): 21--22.

[7] Mana, Antonio, and Ernesto Pimentel. "An Efficient Software Protection Scheme." In Proceedings of the 16th International Conference on Information Security: Trusted Information, 385--401, 2001.

[5] Samuelson, Pamela. "Drm {and, or, Vs} the Law." Communications of the ACM 46, no. 4 (2003): 41--45.

[4] Schneier, Bruce. Crypto-Gram (15th February) [article online]. Available from http://www.counterpane.com/crypto-gram-0102.html#1. Accessed 2003 May 15.

[3] Traw, C, and S Brendan. "Protecting Digital Content within the Home." IEEE Computer 34, no. 10 (2001): 42-47.

[1] Yu, H. "Digital Multimedia at Home and Content Rights Management." Paper presented at the Networked Appliances, 2002. Proceedings. 2002 IEEE 4th International Workshop on 2001.
[6] Zhang, Jian, Yunzhang Pei, and Dong Xie. "A Flexible Content Protection System for Media-on-Demand." Paper presented at the Multimedia Software Engineering, 2002. Proceedings. Fourth International Symposium on 2002.