

©2006 IEEE. Personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution to servers or lists, or to reuse any copyrighted component of this work in other works must be obtained from the IEEE.

This material is presented to ensure timely dissemination of scholarly and technical work. Copyright and all rights therein are retained by authors or by other copyright holders. All persons copying this information are expected to adhere to the terms and constraints invoked by each author's copyright. In most cases, these works may not be reposted without the explicit permission of the copyright holder.

# Digital Cinema Content Security and the DCI

Jeffrey A Bloom  
Thomson  
Princeton, New Jersey

## Introduction

In the summer of 2005, the Digital Cinema Initiative, LLC. (DCI) released Version 1.0 of a specification for digital cinema systems [1]. DCI was a collective formed by the 7 major U.S. studios, Disney, Fox, MGM, Paramount, Sony, Universal, and Warner Bros., to facilitate the introduction of interoperable production, distribution, and exhibition equipment for digital cinema. The resulting specification describes the image and audio formats, compression standards, packaging, transport, theater systems, projection, and security.

Content security is a critical component of a digital cinema system. The content itself consists of high resolution digital imagery ( $2048 \times 1080$  or  $4096 \times 2160$  pixels per frame at 36 bits per pixel) compressed at very high quality (JPEG 2000) and high quality, uncompressed, multi-channel audio (up to 16 channels at 48 or 96 kHz and 24 bits per sample). Being digital, this high quality content is easier and cheaper to duplicate and distribute than traditional film-based motion pictures: both for authorized users and unauthorized users. While the theft of any motion picture before or during the theatrical release window maximizes the damage to the content owners, pirate copies of digital cinema content have the potential to be higher quality (no camcorder required) or cheaper to obtain (no telecine required).

Digital content has a significant security advantage over film-based content. It can be encrypted and thus protected during transport. Intercepted copies of the digital files have little value without the ability to decrypt. DCI has specified very strong, well known encryption standards to protect the content during transport. As is most often the case with content protection systems, the integrity of the security relies on system design, implementation, and key management.

This paper describes the content security system defined in the DCI Digital Cinema System Specification. A more detailed description can be found in [2] and, of course, in the Specification itself. This specification is not a standard and is not a complete specification to which systems can be built. Rather it represents a sketch of how the major U.S. studios would like to see digital cinema systems develop. Many of the ideas in the Specification will be implemented and others will be revised as the motion picture industry adopts and then transitions to digital cinema.

The general topic of digital cinema development is treated well in [3]. Another effort at establishing interoperability in digital cinema is the standards activity within the Society of Motion Picture and Television Engineers [4].

## **Security System Overview**

Digital motion picture content (sound, imagery, and subtitles) is protected during transport from the distributor to the theater by a symmetric key cipher. The encryption allows the content to be safely distributed via any convenient transmission channel including courier, satellite, or computer network. Each motion picture title is encrypted with a different cipher key.

In a separate communication, the cipher key for a particular title is transmitted to each theater authorized to show that title. For this communication, a public key cipher is used so that each theater receives a unique message that can only be deciphered with private keys stored at the theater.

The private theater keys are stored in a secure silicon device that cannot be tampered. In addition to storing the private key, this device, called the Security Manager, is responsible for deciphering the content, decompression (of the imagery), and forensic watermarking of the imagery and audio. This arrangement assures that no adversary will be able to access cleartext, compressed or decompressed, unmarked content without defeating the tamper resistance of the secure silicon or otherwise coaxing out the private key.

The Security Manager will authenticate both the identity and integrity of all downstream security equipment before any output will be enabled. All content communications beyond the Security Manager are over secure (encrypted) channels. Typically, the Security Manager output is sent directly to a Projection System that contains both a projector and interface to the auditorium sound system. The Projection System is housed in a tamper-resistant enclosure and can provide information to the Security Manager regarding the integrity of physical security.

The cipher key used to decrypt the motion picture content is sent to the theaters along with a set of restrictions on how the content can be used. These restrictions are limited to a description of the authorized play window and a list of the authorized devices (security manager and its components and projection system and its components). Beyond that, each exhibitor is expected to use the content in a manner consistent with the negotiated engagement agreement. Rather than enforce the terms of the negotiated agreement with a sophisticated DRM system, the Digital Cinema System Specification defines a secure logging mechanism whereby all use is recorded and later reported back to the appropriate content owner.

## **System Specifics**

### **Transport Encryption**

Digital cinema content is encrypted for transport. Each of the sound, imagery, subtitles is encrypted separately using a symmetric key cipher. More specifically, the data is encrypted using the Federal Information Processing Standard for the Advanced Encryption Standard, more commonly known as AES [5]. This symmetric block cipher is to be used in Cipher Block Chaining (CBC) Mode with a 128 bit key.

## **Key Transport**

The Digital Cinema Package contains audio, imagery, and subtitles, each individually encrypted and delivered, as a package, to each theater. The content decryption keys are then provided as the payload of a Key Delivery Message (KDM), which is sent separately to each theater. The KDM payload is encrypted with the public key of the projector's Security Manager. This insures that only the intended recipient will be able to retrieve the decryption keys. The technology specified for this communication is the RSA Public Key Cipher w/ 2048-bit key [6] [7].

The Security Manager can hold a number of different content keys at any given time. It may need to temporarily cache some of these keys outside of the secure perimeter. All such data will be protected with AES with a 128-bit key or TDES with a 112-bit key [8].

## **Security Manager**

The Security Manager coordinates all auditorium security processes. It authenticates other security devices through the use of digital certificates. Each security device carries a Digital Cinema Certificate defined as a constrained version of X.509, Version 3 ITU standard [9]. This certificate is issued by the device vendor and identifies the make, model, device Universal Unique ID, and device serial number and defines the intended role of the device. Devices can only be used for their intended tasks. Possession of a digital certificate indicates that the device has been certified by the vendor to meet the role requirements.

Part of the KDM payload is a list of trusted devices for the target theater (TDL). This is a list of the specific security devices approved to participate in playback of a particular composition and is created by the composition Rights Owner. The Security Manager is responsible for insuring that only devices on this list can participate in an exhibition of the current content. Thus, a security device may be authenticated as holding the appropriate certificate credentials, but not trusted by a particular content owner. The TDL serves as a mechanism for revocation.

Each security device must be able to monitor its own integrity by detecting tampering attempts and maintenance activities. Upon request, these devices will provide information regarding their integrity status to the Security Manager. Thus, the Security Manager can insure the identity (through authentication), authorization (through the Trusted Device List), and integrity of each device in the security system and can establish secure communications channels with each of those devices.

The Security Manager then establishes a secure Transport Layer Security (TLS) session with each identified, authorized, security device. TLS is a commonly used cryptographic protocol which provides secure communications on the Internet (IETF) [10]. The establishment of a session involves certificate-based authentication followed by public key encryption-based key exchange. The authentication step is that described above.

## **Physical Security**

All security devices are implemented in secure hardware. Secure hardware is hardware with a physical barrier to protect sensitive data preventing access to internal circuitry.

Such hardware should be tamper evident (physical tampering leaves visible traces that can be easily observed upon inspection), tamper detecting (physical tampering causes state changes that can be recorded), and tamper responsive (some action is taken when tampering is detected.)

Some devices, such as the security manager, must additionally be implemented in secure silicon. Secure silicon refers to an IC designed to resist physical and logical attacks with active tamper response that erases all critical security data upon detection of physical tamper attempts.

The DCI Specification provides detailed requirements for physical security, but generally follows the requirements described by the FIPS 140-2 Level 3 Standard (with some exceptions) [11].

## **Secure Logging**

In order to allow exhibitors flexibility in their operations, the content owners have adopted a *Control Lightly / Audit Tightly* approach to security. They have not called for a sophisticated DRM system to manage how content is used. Rather, they specify an exhibition window and a list of trusted equipment. Negotiated business arrangements specify how the content is to be used within that window as they do currently. Exhibitors are responsible for reporting the actual content usage and providing appropriate compensation.

In order to automate this process, the DCI specification calls for a secure logging functionality whereby each security device creates a log of security-related events (including decryption, TLS session establishment, tamper detection signals, etc.) These log records are cryptographically protected against deletion (continuity) and alteration (integrity) and are non-reputable.

## **Forensic Watermarking**

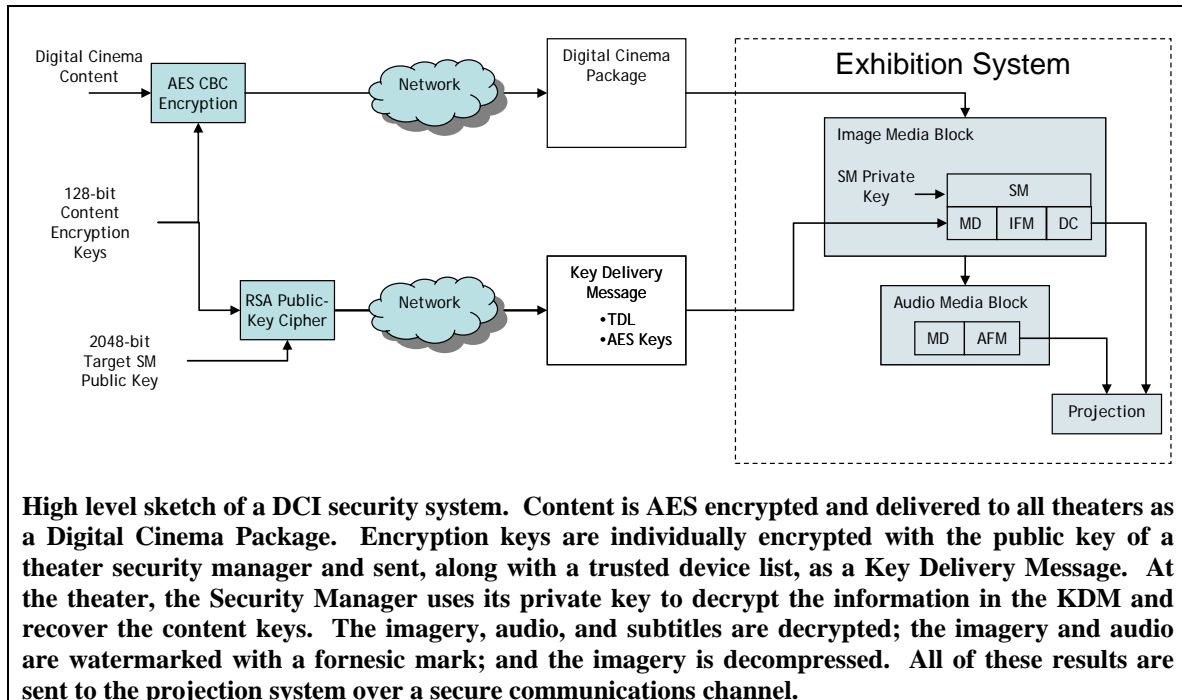
The security devices that perform the decryption of the audio and imagery must have forensic watermarking capabilities. These devices will embed at least 35 bits of watermark payload in each 5 minute block of audio and imagery. Of this 35 bits, 16 bits are used to identify the processing time (16 bits allows for identification of each 15 minute slot in a year) and the remaining 19 bits are used to identify the location of the exhibition. This location could be a unique device identifier.

The purpose of the watermarking is to identify the source of pirated video. Pirated video may be the result of camcorder capture during a scheduled exhibition, camcorder capture during an unscheduled exhibition (no audience), or the result of a successfully undetected tampering of equipment to bypass the security mechanisms. Expert analysts can easily distinguish between these three sources and the watermark payload provides information for further action.

The watermarking technology used must meet very high fidelity standards and very high robustness standards. For example, the watermark payload must be recoverable from a camcorder capture that has been resized to 360×240 and compressed at 500 kb/s or lower as is typical for pirate movies found on the Internet. The watermark must also meet high

security standards as it should not be easily removed or misinterpreted in the face of collusion attacks.

A number of watermarking technologies have been developed to meet these high standards including [12] and [13].



## Summary

The DCI Digital Cinema System Specification of 2005 represents an important step towards establishing an interoperable, secure digital cinema production and exhibition environment. It makes broad use of existing, well accepted cryptographic standards. As digital cinema systems are built and deployed, standards organizations such as SMPTE and ISO will further refine the functionality and interoperability requirements of various digital cinema components.

## References

- [1] Digital Cinema Initiatives, LLC, "Digital Cinema System Specification V1.0", July 20, 2005.
- [2] J. A. Bloom, "Security in Digital Cinema", in *Multimedia Security Technologies for Digital Rights Management*, edited by Wenjun Zeng, Heather Yu, and Ching-Yung Lin, Elsevier, 2006.
- [3] Charles S. Swartz, *Understanding Digital Cinema: A Professional Handbook*, Elsevier, 2005.

- [4] SMPTE DC28.4 Study Group, "SMPTE Digital Cinema Study Group DC28.4 on Encryption and Conditional Access: Interim Report", Release Version 1.0, September 10, 2001.
- [5] National Institute of Standards and Technology, Advanced Encryption Standard, FIPS 197, 2001.
- [6] J. Jonsson and B. Kaliski, IETF RFC 3447, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, The Internet Society, February 2003.
- [7] R. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, 21 (2), pp. 120-126, 1978.
- [8] National Institute of Standards and Technology, Special Publication 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, 2004.
- [9] R. Housley, W. Ford, W. Polk, and D. Solo, IETF RFC 2459, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, 1999.
- [10] T. Dierks and C. Allen, IETF RFC 2246, The TLS Protocol Version 1.0, 1999.
- [11] National Institute of Standards and Technology, Security Requirements for Cryptographic Modules, FIPS 140-2, 2002.
- [12] J. Lubin, J. A. Bloom, and H. Cheng, "Robust, Content-Dependent, High-Fidelity Watermark for Tracking in Digital Cinema", Security and Watermarking of Multimedia Contents V, Ping Wah Wong, Edward J. Delp, Editors, Proceedings of SPIE Vol. 5020, 2003.
- [13] J. Haitzma and T. Kalker, "A Watermarking Scheme for Digital Cinema", International Conference on Image Processing, 2001.