VOL. 11, NO. 9, MAY 2016 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

INFORMATION SECURITY IN D-MEDIA (DIGITAL MEDIA)

S. Balakrishnan[1], A. Jebaraj Rathnakumar[2] and K. N. Sivabalan[1]
[1]Department of Computer Science and Engineering, Sri Venkateswara College of Engineering and Technology, Chittoor, Andrapradesh, India
[2]Deparment of Computer Science Engineering, Karpaga Vinyagar College of Engineering and Technology, Chennai, Tamilnadu, India
E-Mail: balkiparu@gmail.com

ABSTRACT

Many thoughts were taken place to rollout Digital Cinema from Traditional Cinema. Security is perhaps the most important and least understood aspect of Digital Cinema. Adding to the challenge is the uniqueness of the cinema business, making it difficult to have a security model. Information Security interpretation here is in terms of Content Security. The discussion below highlights how Content Security is promised in the world of Piracy.

Keywords: information security, digital media, symmetric, material eXchange format.

1. INTRODUCTION

Cinema Production, whether 35mm or digital, has four main players: the Producer, the Post-Producer, the Distributor and the Exhibitor. The term "Content" will refer to full-length films (either fictional or documentaries). Producer holds rights of the film and the one either the Production House that has bought the right or the Creator of the film. Post-Production isa various stages of intermediate processes accomplished by many different players (labs and post-production houses).
The main post-production steps are:

Lab processing: Major portion of the cinema is still shot in 35mm negatives; a first step is needed to develop these films into a film positive.

Film-to-tape transfers: The process of transferring film positive to tapes.

Off-line editing: It's majorly a creative step after the shooting, and done in close relation with the film director. This is a process of assembling the original filmed footage into a rough cur film version.

Scanning and lossless file transfer: It's the process of creating lossless digital files from analogue support.

Dust-busting: The digital enhancement technique is processes at getting rid of dust and speckles resulting from the scanning process.

Compositing and special effects: It's another digital enhancement technique aimed at creating effects that were not possible during the shooting. It superimposes different layers to create a final enhanced scene.

Colorimetry (Color Correction or Grading): The process enhances the rough cut by changing lighting and color throughout the film, either to create an artistic effect or to homogenize lighting in different shots corresponding to the same scene.

Title generation: This step creates the opening and closing credits.

Dubbing and/or subtitling: These processes create a synchronized audio or text translation of the film dialogues respectively, to integrate into the film when needed.

Mastering: It's about creation of final lossless copy of the film to be archived and also for different purposes.

Disk-to-film transfer and printing: This process is the symmetric of the scanning step; it converts the final digital material into 35mm copies.

The above steps were integrated into single post-production houses, depending on their size.

Distributor: It is the intermediate player, the link between the producer and the exhibitor. This role is very often much more than a mere logistic intermediate and embodies the rights holder of the film with regard to the exhibitor. The distributor is the one who does negotiation with exhibitors. The contract settles the time-window during which the exhibitor is allowed to play the film.

Exhibitor: It is the last player in the process, who aimed to project the content to the public.

1.1 Changes with Digital Cinema

The customary movies have been appropriated on the film and demonstrated in motion picture houses far and wide with film projectors. Motion pictures now can be digitized and displayed on new computerized projectors like those utilized for anticipating PC presentations. The new projectors can extend high-resolutions symbolism to a screen more than 100 feet away. Together, circulation of film in a computerized arrangement alongside the utilization of an advanced projector is called Digital Cinema. With the quick improvement of advanced innovation, Digital silver screen outflanks traditional films and pulls in the motion picture industry. Computerized innovation adjusted in the entire film making process has tackled numerous basic issues before: muddled innovation, troublesome storage, abrasion and maturing, environment contamination, high cost etc.

The computerized silver screen substance is put away with the advanced media, transmitted through physical media, satellite or virtual private system. The greater part of the transmission ways are shoddy and convenient, besides, being advanced, the silver screen substance are less demanding and less expensive to copy than traditional film-based movies. So as to ensure the guarantor's legal advantages and advance the sound

development of computerized silver screen, some control measures must be taken to guarantee the computerized content safe. Digital substance has a huge security advantage over film-based substance. It can be crypted and consequently ensured amid transport. Blocked duplicates of the advanced documents have little value without the capacity to decode.

2. DIGITAL CONTENT ENCRYPTION

The key need in security is to conceal data from unessential aggressors. This requirement has brought forth various types of cryptographic primitives including symmetric and asymmetric cryptography.

Symmetric cryptography: In symmetric encryption, a key is share between the sender and the receiver which is kept mystery from the interloper. Among the various types of symmetric algorithms, Advanced Encryption Standard (AES) [1] is picking up notoriety because of its preferred security and effectiveness over its forerunners. AES standard could bolster 128 bits length piece size and128, 192 and 256 keys the subsequent calculations are named AES-128, AES-192 and AES-256respectively to demonstrate the length in bits of the key. AES is in light of S-P arrange in which the whole 128 bits data square is composed as 4*4bytes cluster called State and is handled in a few rounds. Security of AES ought to be considered in three perspectives: savage power assault, scientific assault and timing assault. An incredible many experiments demonstrate that no real security assault has been demonstrated fruitful against the AES till now.

Asymmetric cryptography: Unlike the symmetric cryptography, uneven cryptography uses a couple of keys to encode and decode message. One of these two keys is known as pubic key as it is disseminated to others and the other is called private key which is kept mystery. Normally public key is utilized to encode any message which must be unscrambled by the corresponding private key. RSA is the most broadly utilized awry encryption framework.

In RSA, the plaintext and the cipher text are considered as integers between 0 and n-1, where n is the modulus. The security of the RSA cryptosystem is not perfect, but this can be prevented by increasing the length of key as security of actually dependent of the difficulty of finding prime factors of it. It is recommended that the size of modulus is 2048 bits. However, more bits in the key, more slow to generate it. By comparison, it is known that AES algorithm has high efficiency, fits for large data blocks encryption, but the secret key distribution is considered as a critical issue. As an asymmetric cryptosystem, RSA solves the problem inherent distributing the secret key. The major drawback of RSA is its greater computational overhead due to its large key. Hence, the probable solution is the use of a hybrid encryption system in which typically AES is used to encrypt large data block (video and audio MXF files in our system) and RSA is used for the key management and digital signature applications.

2.1 Digital certificate

As specified past, RSA [2] open key could be available by anybody, who can get the public key from a Digital Certificate. Digital Certificates are the electronic partners to driver licenses, travel papers and membership cards, tie a personality to a couple of electronic keys that can be utilized to scramble and sign digital information. Digital Certificates utilized as a part of a D-Cinema framework [3] are taking into account a compelled type of theX.509v3 organization and preparing guidelines, help secure interchanges both inside of an exhibition facility and between business elements (Studios, Distributors and Exhibitors). A Digital Certificate for a security gadget is an announcement marked by the merchant of the gadget, and makes it conceivable to verify the gadget that it has the privilege to utilize a given key, serving to keep individuals from using phony keys to mimic different clients. The assortment of endorsement records properties, for example, the make, model and serial number of the gadget, and the D-Cinema parts bolstered by the gadget.

A Digital Certificate is issued by a Certification Authority (CA) and marked with the CA's private key. For reasons of scaling and security, gear merchants require not straightforwardly sign the certificates of gadget. Rather there may be one or more transitional declarations in a chain. The vendor's essential authentication is the "root" of this chain (called the root testament), and the device's certificate is the "leaf-end" of the chain. People in general key in the merchant's root authentication (which is self-marked) may be utilized to confirm the characteristics in a moderate endorsement. Those attributes include people in general key of the moderate CA, which is then used to check the following endorsement in the chain, et cetera. In the long run, the general population key from the last CA declaration in the chain is used to confirm the gadget's endorsement, and in this manner set up the dependability of the characteristics in the certificate (counting the gadget's open key).

2.2 Material eXchange format

The Material eXchange Format (MXF) [4] is an open file format, targeted at the interchange of audio-visual material with associated data and metadata. It has been designed and implemented with the aim of improving file-based interoperability between servers, workstations and other content-creation devices.

An MXF file starts with a File Header, is followed by a File Body and is completed by a File Footer, as shown in Figure-1, just like a wrapper intended to encapsulate and accurately describe one or more “clips” of Essence. These Essence “clips” may be Pictures, Sound, Data or some combination of all of these. Every item in an MXF file is KLV-coded. This means that every item within the file is identified by a unique 16-byte key and by its length. Each plaintext triplet is designed to be processed independently, so does the encrypted triplet, allowingencryption/decryptionto start anywhere within the Track File.

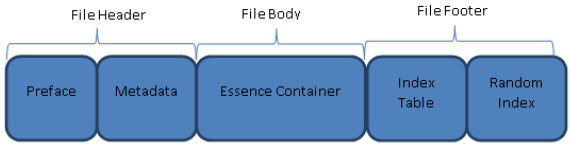

Figure-1. Data structure of MXF file.

Correspondence between Source and Encrypted Triplets is shown as Figure-2.

K	L	V

PlaintextTriplet

K'	L'	CryptInfo	K	L	E(V)	CryptInfo

Encrypted Triplet

Figure-2. Correspondence between source and encrypted triplets.

The value V of a source plaintext KLV Triplet is first encrypted to yield E (V). The encrypted value E (V), along with K and L, is wrapped in a K'L'V' Encrypted Triplet. K' is a unique label common to all Encrypted Triplets, independent of their content. L' refers to the full length of V'.

V' consists of K, L and E (V) from the source Triplet as well as cryptographic information specific to the Encrypted Triplet. This cryptographic information includes the initialization vector used in generating E (V) and the message integrity code used to verify the integrity of the Triplet.

2.3 Key delivery message

Key Delivery Message is a key file in the Digital Cinema Package (DCP). D-Cinema systems require that content keys (encrypt the plaintext in the MXF file), key usage time window (key parameters) and "trusted equipment" information (Trusted Device List or TDL) be communicated to exhibition facilities. The KDM carries all the critical information required to enable content decryption according to a baseline interoperable security standard. The basic form of the KDM is shown in Figure-3.

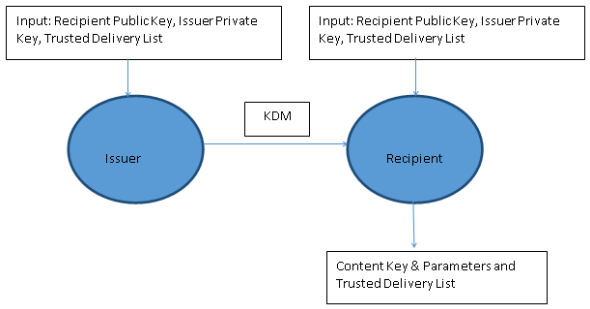

Figure-3. KDM Information flow.

The KDM uses XML [6] [7] to represent the information about content decryption keys and provides security using the XML Encryption and Signature primitives. The relationship between the KDM and the Composition Play List (CPL) [9] is shown in Figure-4.

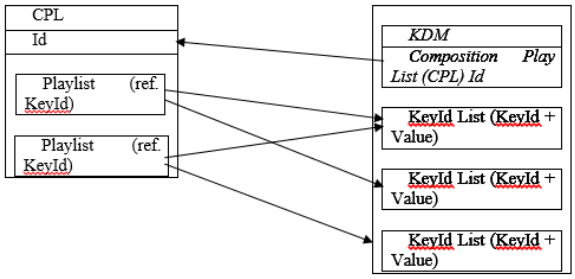

Figure-4. Linking between CPL and KDM structures.

Access to the full information payload of the KDM requires knowledge of the targeted recipient's private key (Key Value in Figure-4). Having this key, the legitimate recipient may unlock and validate both encrypted and plain text information contents carried. Normally Digital Cinema issuers provide a Key Delivery Message bundle (KDMb) file to each Cinema rather than sent a KDM respectively to its owner. The KDMb is a compressed archive that contains a mapping file and a directory containing a collection of one or more KDM files afterward every recipient can distinguishes and extracts his KDM automatically.

3. DIGITAL CINEMA SECURITY SYSTEM

Section 2 introduces the most pivotal part in the system, but it is not enough for integrality. Other parts also play important roles.

The following diagram describes how the system works. Define some acronyms used in the Figure:

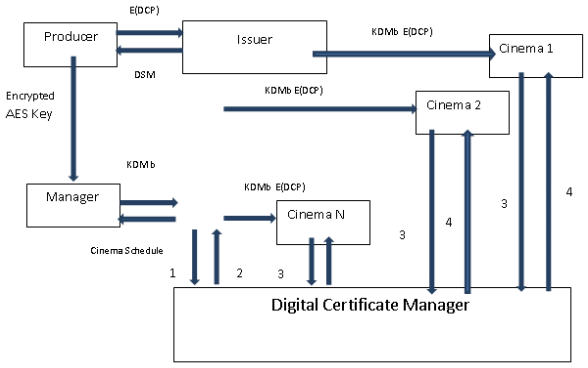

Figure-5. Digital cinema security system workflow diagram.

E(DCP): Encrypted DCP

1: apply for certificates of Cinema 1 to Cinema N.
2: offer certificates of Cinema 1 to Cinema N.
3: apply for certificate of Issuer.

4: offer certificate of Issuer.

They act like this:

Digital certificate manager: A multilevel structure, to issue root, secondary and leaf certificates.

Digital cinema producer: to be responsible for post-production, image compression, packaging, producing encrypted DCP.

Digital cinema issuer: provides Producer with Digital Source Master (DSM) manages D-Cinema information, including basic information and movie valid dates, also takes charge of issuing D-Cinema by sending encrypted DCP binding KDMb to Cinemas authorized.

Digital cinema manager: in charge of generating KDMb with AES key sent by Producer, cinema schedule from Issuer and TDL in his own database.

Cinemas: get the decryption key from the right KDM and unlock the encrypted DCP for projection.

4. CONCLUSIONS

A Digital Cinema Security System has been designed, covering the entire process from post-production, image compression, packaging, encryption, certificate authority, cinema information management. Advanced Cinema offers the motion picture industry the potential of increased security and accordingly, diminished theft rates. Encryption and standard DRM conventions can ensure the movement picture when away and amid travel from one procedure or location to another.

REFERENCES

[1] 2001. AES Specification. Federal Information Processing Standards Publication. p. 197.

[2] B. Kaliski. 2003. PKCS #1: RSA Encryption Version 2.1. IETF RFC 3447.

[3] 2006. The Society of Motion Picture and Television Engineers. D-Cinema Operations Digital Certificate.

[4] The Society of Motion Picture and Television Engineers. SMPTE - MXF File Format Specification.

[5] 2001. The Society of Motion Picture and Television Engineers. SMPTE 336M-2001, Data encoding protocol using Key-Length-Value [S].

[6] 2002. XML Encryption Syntax and Processing. World Wide Web Consortium December.

[7] 2002. XML Signature Syntax and Processing. World Wide Web Consortium December.

[8] www.w3.org/TR/2002/REC-xmldsig-core-20020212.

[9] 2007. The Society of Motion Picture and Television Engineers. SMPTE 429-8 D- CPL Playlists [S].