

DC28.4 and DC28.5 Digital Cinema Study Groups Comments

DC28.4 Digital Cinema Encryption/Conditional Access

DC28.5 Transport Study Group

Purpose

This study looks at the transmission and protection of the Digital Cinema Distribution Master through the distribution system from the Studio and the Theater sites. It will look at protection and tracking methods including potential methods of reducing losses if the work is stolen and reproduced by pirates.

The only proven way to absolutely guarantee that a movie property, whether film reels or DCDM, will not be stolen is to never distribute it, or show it. This technique, though effective, provides considerable strain on the economic model of the industry.

A method of reducing property loss and limiting ROI exposure will be examined. This methodology requires that a value can be placed on the movie property at different parts in its distribution life.

An interface definition is first proposed to specify the distributor output port and theater site input port.

Common Socket at Distributor output and Theater input

The Distributor Output of the DCDM to the transport system and the Theater site Input of the identical DCDM from the transport system is most easily and flexibly defined as an "RJ45" connected with 10BaseT/100BaseT/1000BaseT Ethernet connection with IPV6 addressing. All systems discussed below can be easily described as to and from such a connection.

Protect the Owners Value of the Digital Movie Property

A method of valuation of the DCDM, or film print, of the property is needed to be able to judge the loss at any time during the life of the property. This value could then be insured or bonded. Insurance companies and bonding agencies familiar with the industry would insure or bond to the current value and risk of loss from this location.

Traceability of the loss to a specific copy, and the responsible party, should yield lost revenue recovery, to the IP (Intellectual Property) owner.

Responsibility

To clarify the discussion it has been assumed that the Distributor is distinct entity from the Production Studio. If the Studio chooses to do the distribution directly, then the distributors function responsibilities are merged into the studios responsibilities.

The Studio's Responsibilities

Protection of the Digital Cinema Master Database – This database is kept in the vaults of the production studio. While in the vaults, and in the required daily use of the digital images, reasonable efforts must be made to insure the safety of the property. This supposition would expect the working images and sound to be encrypted and strong key control implemented. The studio would be responsible for losses at this stage of the properties life.

Protection of the Digital Cinema Distribution Master – This database is sent to the distributor for redistribution to the theaters. Each copy sent to the distributor should be watermarked and encrypted for the distributors use. Traceability must be established to be able to track any potential loss mechanism.

The Distributor's Responsibilities

Protection of the Digital Cinema Distribution Master – Each distributor will receive the input copy from the studio, with the studio-distributor watermark, will then add the distributor-theater watermark and encrypt the modified database with a key specific to that theater site. The key is then encrypted with a public key cryptography to be sent to the theater site. The main distribution of the DCMD is via the methods shown below.

The Theater's Responsibilities

Protection of the Digital Cinema Distribution Master – This master must remain in it encrypted mode throughout its presence in the theater except for the frame by frame decryption, decompression, conversion for device, local watermark addition, compression and local encryption process, to the Display Working Copy for storage in the main server or high speed video server at display device. The content is exposed only for the time required to convert a frame.

DC28.4 and DC28.5 Digital Cinema Study Groups Comments

Protection of Display Working Copy, DWC, of the movie property – Each DWC, converted for the display mechanism requirements and imperfections, will be decrypted and uncompressed, at or near the projector/display device as being shown.

Methods

Encryption

The most secure encryption systems are those systems with the most crypto analysis targeted on them without weaknesses found. An encryption algorithm can only be rated as strong when it cannot be successfully attack with: 1) Its algorithm made publicly available; 2) a complete description of how it works; 3) how the keys work. It must be tested with all know cryptographic attacks and survive without a blemish. The current finalist for the National Advanced Encryption Standard from the National Institute of Science and Technology have passed most of that screening, I will use the TWOFISH algorithm in the descriptions here as it is IP free and has been placed in the public domain. This algorithm uses a 256 bit key and mean time to successful attack is in the order of 10^{20} Years. Encryption speed is 18 Pentium clock cycles per byte or 55.5Megabytes per second, 30 minutes/100GB DCDM, on a single 1GHz processor. Multiple parallel processor can be applied to speed the process of encryption and decryption if needed. A test of the encryption system is proposed.

Distributor to Theater

Most Secure System – Each transfer is individually watermarked and encrypted uniquely for a given theater site or theater screen. This means each transfer is a different copy of the DCDM and hence transferred individually. The lowest cost of such a transfer is \$40.00/DCDM using readily available current technology with the cost decreasing in future.

More cost effective system – This system would reduce the amount of material that is individually watermarked to 1% or 10%. This could be just the center pixels of each image or a strip through the image or some other visually obvious missing part. The bulk would be sent via a common encryption key and watermark to all theaters via satellite or DVD and the smaller section would be sent via the FTP system. If the satellite system were used for 99% at \$3.70 and the remainder sent via FTP over DSL for cost of \$0.40 the distribution cost could be as low as \$4.10/DCDM now for a large distribution. Please see attached spread sheet.

In Theater Systems

The strength of this system would be the subject of contract and security concerns of the insuring agency or bond poster. A very secure system has been described. Supervision by the distributor and insurance/bond provider will be used to support contractual requirements

Assumptions

Any Transmission Method will be intercepted - All transportation of the movie database must be protected by encryption. Any transmission can and will be intercepted. The only safe assumption to make is that the first copy sent is intercepted by the party that could cause the most damage. All transmitted Encrypted Keys are intercepted - This is a standard assumption and the key distribution system must take it into account and is corollary to the interception of the transmitted data.

Must Have Guaranteed Delivery - For a successful distribution, there must be a reasonable delivery guarantee. Both a primary and a secondary distribution method must be in place. All transactions are described by contract - All business with respect to the distribution and exhibition of a theatrical property is by contract that will take precedence to any discussion here. The rules change with each contract.

Trailers and Commercials are treated the same as the DCDM for transport purposes. I would expect that trailers and commercials would be made available on the web for advertisement purposes.

Theater sites will need to perform work on the DCDM for use in the chosen display device. This will require access to the pixel information “plain text” to convert for: 1)Color space of the Display device; 2)Correct for display physics, such as keystone effects; 3)Correct for the gamut of the display environment; 4)Lens non-linearity, spectral and linear imperfections corrections; 5)Mapped non uniform response of each display pixel element; 6)Pixel aspect ratio changes from

DC28.4 and DC28.5 Digital Cinema Study Groups Comments

DCDM aspect ratios; 7)Map sound to match ITU specification, which may changing channel sound delays; 8)Map sound channels for flattened acoustic properties; 9)Local watermarking with screen and time information; 10)All the other stuff forgotten in this quick response. While some of these corrections may be applied at image display time, some may require significant preprocessing beyond the scope of the projector. The results of the displayed image must be measured, spectrographically and audio imagery, and compared with the DCDM to demonstrate the correct interpretation of the DCDM.

Once a DCDM is sent, this process cannot be revoked. We can update keys to allow showing at specific time periods in the future. We can require a certificate of compliance on the removal of the DCDM copy. We cannot recall that which has been sent. We do not have to send the Key. Someone is almost always responsible for the loss of the film or DCDM file.

Current Film Practice

Thanks to Carol Hahn of Qualcomm and Mike Jones of Sony for this information. A much more extensive and through presentation is being prepared by Mike Jones.

If the averages are used the cost of a print to a theater, ready to show, is about \$1550 and the preparation time is about 4 weeks from start of production to first opening.

From SMPTE SF meeting the average cost of projection is about \$19.00 for film.

Yearly "movie" production

Approximately 400 productions yearly – major Studios

1 – 10,000 productions – TV and Independent producers

Theaters

US = 37,000 Screens - World Wide = 110,000 Screens

The largest multiple screen theater complexes have up to 30 screens.

There are 7,551 theater sites in US

A screen may do 25 movies/year

Target distribution - Godzilla

Largest attributed single release to date – Godzilla.

Cost per print - Varies with number of prints and length of print with an average of \$1500 per print.

Time to make prints - Varies with length of print - 3wks for Godzilla. The average lab print capacity to a single film is about 300 per day.

Theaters want the film 2-3days in advance to verify and prepare for showing.

Transportation cost per print is based on weight, 50 to 70 lb, and the speed required from slow owned truck to courier with a range of \$25 to \$400. For the purposes of this paper we will assume an average of \$50.

Total cost per print delivered to theater for comparison purposes = \$1,550.00.

Current Loss Mechanisms

Camcorder off screen in theater – better cameras make better copies

“Borrowed” print from theater – Duped or scanned

Copy Stolen in transit – Duped or scanned

New Distribution Methods

All methods described here assume a 100Gbytes of delivered data. Current digital cinema is about 55Gbytes with 12 channels of 96000 samples per second 24 bit uncompressed audio. This allows for long movies with extensive audio support. For most security and tracking purposes, each copy is individually watermarked and all contents encrypted.

A large saving in cost can be achieved by using a common encryption on most of the movie and individual encryption on 1 to 10% of the movie. This would allow up to 99 gigabytes to be sent via satellite and the remaining 1GigaByte to be sent via Internet or individual DVD RAM or other distribution media.

The encryption used should be one of the five proposed for the new AES (Advanced Encryption Standard). For this paper we will consider TWOFISH as the encryption method.

For Cost of Transfer Comparison

Large Distribution = 6700 copies (print equivalent)

Small Distribution = 100 copies (print equivalent)

Transfer is non-realtime except as noted

Display Corrections will be made at theaters

Database servers exist at distribution points

DC28.4 and DC28.5 Digital Cinema Study Groups Comments

Database servers exist at theaters

Video system at theater dependent on viewing method

Average Theater site has 5 screens and would take 10 DCDM's per month

Magnetic Tape

Using AMPEX Data systems Quad Density DST tape technology, cost data provided by Don Hennessey, and Ampex DST 312 tape drive, the cost of a small 100GB cartridge is about \$140 and down to \$99 in 6000 volume, delivery \$5 to \$20 FedEx. With a write speed of 20MB/second each tape takes 1.4 hours. Assuming machine cost of \$6/hour the production cost is \$9. Cost delivered to theater is \$275 max including equipment lease.

Reuse of the media for 20 times would bring costs down to \$5 for media and \$20 for writing and shipping for a total \$145 to theater.

The tape drive will cost about \$129,000.00 initially and ~\$65,000.00 if high volume is reached which would be about \$3200/month initially, and \$1600/month in volume, leased. For a standard theater site using 10 movies per month the cost is \$160 to \$320 per movie.

Other tape systems may have merit such as 8mm, 4mm and DLT tapes with much lower machine costs while the tape cost are about the same.

DVD RAM

Each DVD RAM is about 4.6GBytes. This would require 25 disks at a cost of about \$40/disk for a cost of \$1000. The delivery cost is \$5 to \$20 and the writing cost is about \$5 per set. Total cost to theater is \$1030. This media is reusable and could be recycled. If media is reused 20 times the cost is reduced to \$40 + \$10 or \$50 total.

DVD ROM as a mass produced media is not useful for single individual copy production.

If trace ability is not required, DVD ROMs at 18GB per disk would probably cost about \$49.90 to press, and ship, per set.

Hard Disk

Current Hard Disks are about \$750 to \$3300 for 3 drives at 36GB each. New disks from IBM are 211Gbytes each. The backup delivery system is the Distributor sales person with 8 disks in a special briefcase that can be plugged into the RJ45 interface point. The major cost is person carrying the brief case. Transfer time for movie to theater is about 45 minutes per movie.

Satellite download

Satellite download are available from several vendors. The data used here is from the Echostar business data delivery service per Doug McGary of Echostar.

Real time transmission at the higher data that we will be displaying will require 18 of the satellite data channels with a throughput of 55.2Mbit/second with an associated cost, on a monthly basis of \$3.6M or \$50K/hour.

Direct T1 to OC12 Connection

Pricing on T3 and OC3 lines per Vince at PacBell for installation in California.

Equipment costs are included in a 5 year lease program.

The higher data rate lines are dominated by the cost of the line that would require a large number of screens to justify.

Internet Delivery

DSL connections are the cheapest at \$39.58 including equipment costs for the distribution of the DCDM.

If it is decided that we can ship only 1 to 10 percent with specific watermarks then a combination of Satellite or DVD and Internet DSL is the lowest cost.

DirecPC offer a similar to the Internet delivery except via satellite. This would be a good alternate method where DSL is not available due to telephone line and switch conditions.

History/Future

Telecom speeds

Telecom cost for data transfer have decreased from 110 baud @ \$3/minute on 1975 to 6000000 baud @ \$0.44 per hour in early 2000 or from 220 bytes/dollar to 4.875

Gigabytes/dollar roughly 22 Million to 1 in 25 years. This is a 34% per years decrease in cost over 25 years! There is not reason to assume a change in this price decline.

Other Technologies

DC28.4 and DC28.5 Digital Cinema Study Groups Comments

With film and satellite as probably the only raising costs and DVD declining at only 6% per year, the cost of the distribution is decreasing at about 25% to 35% per year. The cost of shipping the media dominate the total costs at the 5 to 10 year points.

Testing the System

The strength of the distribution relies on the security of the encryption system used for the distribution to the theaters and for storage at the theaters. A much-repeated cry is the fear of the attack and theft of the D-Cinema property by “Hackers” and professional thieves. This process should be monitored and validated by the studio security and with the help of external Security specialist like RSA associates, PlusFive Consulting or Counterpane consulting. Working with the NIST people would be useful.

This proposal of for two tests to 1): Test the DCDM distribution system and 2) Test the distributor and theater storage server systems.

Transport Encryption

One way to test the distribution security is to encourage attacks and attempted thefts and pay a reward if any person is successful. Publish several short (3 frame) test images and the encryption algorithm and the encrypted public key and see if they can be broken.

Build a set of test images

Build a set of test images consisting of three frames, title frame, one unique frame from movie, and one instructions frame. The instruction frame would have a unique number for verification and where to call, fax or email the clear test frames. Watermark the set of frames.

This should be a group of 25 or 30 sets of image sets based on a set of motion picture properties from each studio. The reason for building a large set is that once they are encoded, the selection process will insure that no person knows which ones are used for the second part of this proposal.

Encrypt with AES candidate algorithms

At the time of this writing there are five finalists in the Advanced Encryption Standard competition being sponsored by the National Institute of Standards and Technology: Twofish, RC6, MARS, Rijndael, and Serpent. These are all much stronger than the Triple-DES algorithm.

For details see <http://csrc.nist.gov/encryption/aes/round1/r1report.htm>.

These Encryption standards all use up to 256 bit keys which in general puts the average time to break the key at greater than 10^{20} years with a well funded attack. The source code and algorithms for all the candidates are published, are well studied and understood. Secret algorithms are never to be trusted.

Encrypt the candidate test images using the Twofish algorithm, alternately use all 5 different algorithms, and publish the encrypted copy to each potential hacker or breaker. For Twofish see <http://www.counterpane.com/twofish.html> for details and source code. Unoptimized C code runs at about 500 clocks per byte on a Pentium and optimized assembler code run about 18 clocks per byte on a Pentium processor.

Create a temporary distributor and temporary theater and create a public key pair for each and use this to encrypt the keys for the 5 samples. Publish the public keys for the distributor and theater and the public key encrypted traffic with the key for the test images. Use a 4096 bit public key such as PGP or RSA.

Offer prize for solution within 6 month window

Post a prize for anyone that can bring/send copies of any of the encrypted movie frames of \$1 Million. They must also show how they broke the code and the techniques used (prevent fraud) and the unpublished watermark will be checked. Offer a part in a movie or, something else to appeal to the ego, and get them working on breaking the code.

To add spice put the Prize money on a decreasing value basis to mimic the changing value of the movie that it would protect.

Theater Storage Systems

This will provide a similar result to the above test and check the security of a well prepared theater storage system.

Build a typical theater storage systems

DC28.4 and DC28.5 Digital Cinema Study Groups Comments

Build a storage system with the remainder of the trial 3 frame sets, and use the same encryption described above to store the data on disk.

Use a test theaters

This should be at a test location as it will be a large target and will be under attack almost continuously.

Leak the web addresses

The idea is to be public and subject to the rash of attacks.

Issue challenge to hackers and reward

Post a financial prize, and an ego prize for successful penetration and theft of a movie image set.

Conclusions

Distribution costs from the distributor to the theater for individually watermarked and individually encrypted 100 GigaByte DCDM's can be as low as \$40.00. If only 1% of the film is watermarked and individually encrypted, common encryption used on the remaining 99%, the cost of a joint satellite and internet solution is about \$4.10. Bits are not free but are not terribly expensive. Building 4K by 4K pictures and later 8K by 8K is not a transport cost issue. Please note the decreasing cost estimates on attached spread sheet. Newer methods of distribution will constantly be available and should be embraced as they become cost effective.

A common interface portal for distribution has been defined as 10/100/1000 Megabit/second Ethernet connection with IPV6 addressing is a very common and easily configured solution. Watermarking adds the "serial number" required to be able to trace the source of loss of the property. Encryption with NIST AES candidate algorithms and public key distribution systems insures accurate delivery and verification. Encryption and storage methods must be tested to give confidence to the system. The proposed method should flush out any weakness in a very concentrated attack on the system. Theater control mechanisms have been suggested and can only be guaranteed by making the Theaters responsible through insurance policies and bonds for the property they hold. This also leads to supervision by the insurance company and bonding agencies based on risk analysis. Let's make the best possible movies and display them in the best possible manner. All the systems described here have the inherent ability to trickle down to smaller audience systems.

Respectfully Submitted

Bob Davis
Summit Computer Systems, Inc
22685 Summit Road
Los Gatos, CA 95033-9310
408-353-2706
bob@scsi.com