MovieLabs Specification for Enhanced Content Protection – Version 1.0

Introduction

Digital content distribution technologies are evolving and advancing at a rapid pace. Content creators are using these technologies to produce and distribute increasingly compelling and valuable content for consumers. Unfortunately, digital content distribution also involves substantial risks of unlawful reproduction and redistribution of copyrighted works. Accordingly, MovieLabs believes that increasingly sophisticated content protection is critical to the viability of these technical and creative advances. We also believe the technologies described in this specification should be integrated into products such that they are transparent to the user.

This document describes a set of high-level specifications for improving the security of audiovisual works in this developing environment. These feature specifications are not intended to be static, but rather to evolve as the available technology evolves. Although the applicability of some features may vary by situation, MovieLabs recognizes that most of these features will have broad and strong studio-wide support in most contexts involving enhanced content distribution. Each studio will determine individually which practices are prerequisites to the distribution of its content in any particular situation.

Notice

Motion Picture Laboratories, Inc. (MovieLabs) is the author and creator of this specification for the purpose of copyright and other laws in all countries. The MovieLabs' copyright notice must be included in all reproductions, whether in whole or in part, and may not be deleted or attributed to others. MovieLabs grants to its members and their business partners a limited license to reproduce this specification for their own use. Others should obtain permission to reproduce this specification from MovieLabs.

This document is intended solely as a guide for companies interested in developing secure products. Each MovieLabs member company shall decide independently the extent to which it will utilize, or require adherence to, these specifications. All questions on this topic and the specifications must be independently directed to individual MovieLabs' member companies. MovieLabs shall not be liable for any exemplary, incidental, proximate or consequential damages or expenses arising from the use of this document. This document defines only one approach to security and compatibility, and other approaches may be available.

This document is an authorized and approved publication of MovieLabs. Only MovieLabs has the right and authority to revise or change the material contained in this document, and any revisions by any other party are unauthorized and prohibited.

Compliance with this document may require use of one or more features that may be covered by proprietary rights such as patents. MovieLabs takes no position with respect to the validity or infringement of any applicable proprietary right and it expressly disclaims any liability for infringement by virtue of the use of this document. MovieLabs has not and does not investigate any notices or allegations of infringement prompted by publication of any document, nor does it undertake a duty to advise users of its documents of such notices or allegations. MovieLabs expressly advises all users of this document to investigate and analyze any potential infringement situation, seek the advice of intellectual property counsel, and, if appropriate, obtain a license under any applicable right or take the necessary steps to avoid infringement. MovieLabs respects the intellectual property rights of others and expressly disclaims any intent to promote infringement.

Problems/Threats

The goal of enhancing content protection is to mitigate certain piracy problems that are not adequately addressed by current practices and to prevent piracy problems that might occur in situations when there are multiple formats and means of distribution carrying the first high quality targets each exposed to different threats.

Availability and Distribution of Ripping Software

Ripping applications appear from time to time, sometimes working across a sufficient footprint with sufficient reliability to be viable as illegal software products. This is enabled by two “hack one, hack all” scenarios. First, breaking protection on one device, e.g. a PC + drive combination, breaks it on a wide class of devices. And second, breaking protection on a new title often requires no additional information or technology than breaking it on a recent, previous title.

Release Day Availability of Rips

Often, pristine, pirated copies of the original compressed video are available as soon as the title is released. This is enabled when ripping a new release requires no additional information or technology than ripping a recent, previous one.

Pre-Release Day Availability of Rips

With content released on discs, often pristine, pirated copies are available even before the release. This is enabled by the above, plus leaks in the physical supply chain.

Output Capture

Hardware devices and software applications can often capture digital, baseband video imagery. In the case of hardware, this is enabled when the hardware protection or hardware supply chain has been compromised. In the case of software, it is enabled when a secure media pipeline is compromised. While ultimately camcording the screen cannot be prevented, it can be addressed by forensic watermarking.

Of the threats above, the availability of release day rips is the most challenging to prevent because it only takes a single skilled adversary with a single compromised platform to post a single copy to a file-sharing network.

DRM System Best Practices

Cryptography

- The system shall use state of the art cryptographic functions, e.g., a cipher of AES 128 or better.
- The system shall be resistant to side-channel attacks.

Connection

- The system shall allow the content provider to hold back the delivery of license keys to the device until the street date.
- Systems supporting copy or move shall require the license to be re-provisioned through an on-line process that is performed using keys not present on client devices after a copy or move.

Hack One, Only Hack One

The compromise of security on one platform shall be limited to that platform. And the compromise of security on one distribution of a title shall be limited to that distribution.

Binding to Device

- The system shall bind the ability to decrypt a license key to a particular device (host and/or storage). License keys shall be encrypted such that they cannot be decrypted without the keys of the individual device for which the license was issued.
- The compromise of the keys for a set of devices shall not make it easier to derive the keys for another device.

Software Diversity

- Systems relying on software that is potentially subject to attack shall be implemented in diverse ways so that an attack is unlikely to be portable. This diversity shall vary by version of the system, by platform and by individual installation.

Copy & Title Diversity

- The content protection system shall provide capabilities so that in the event of a breach on one title or version of a title, additional work is needed to breach the content protection on the next title or another version. (N.B., simply using different content keys is not sufficient to satisfy this practice.)

Revocation & Renewal

- The system shall have the ability to revoke and renew versions of its client component.
- The system shall have the ability to revoke and renew code signatures if these are used as part of the system's root of trust.
- The system shall have the ability to revoke individual devices or classes of devices.
- In the above cases of revocation, the system shall support an alternative to that allows access to alternate content or only to existing purchases.
- The system shall proactively renew the protection and diversity of its software components.
- The security provider shall actively monitor for breaches.

Outputs & Link Protection

- The system shall allow HDCP 2.2 or better to be required by content
- The system shall allow other outputs to be selectable by content.

Platform Best Practices

Encryption

- The platform shall support a stream cipher of AES 128 or better
- The platform shall be resistant to side-channel attacks
- The platform shall support a true random number generator

Secure Media Pipeline

- The platform shall implement a secure media pipeline that provides end-to-end protection that encompasses, at a minimum, decryption through to protected output. This secure media pipeline shall include protecting secrets (including keys and derivative key material) and both compressed and decompressed video samples from access by any non-authorized source.

Secure Computation Environment

- The platform shall support a secure processing environment isolated by hardware mechanisms running only authenticated code for performing critical operations. The security of this environment must have been proven with extensive testing.
    - E.g., secure OS, media pipeline configuration, handling sensitive cryptography
- The platform shall be able to protect memory of the secure execution environment against access from untrusted code & devices.
- The platform shall support runtime integrity checking of secure applications.

Hardware Root of Trust

- The platform shall support a secure chain of trust for code that executes in the secure execution environment. The root of this trust shall be securely provisioned, e.g., permanently factory burned.
- The platform shall support a device-unique private key for protecting stored secrets. It shall be:
    - securely provisioned, e.g., permanently factory burned using encrypted communication in the facility so that keys are not revealed in network or other operational logs,
    - usable in certain crypto ops, but never visible even to trusted software,
    - usable (as a means to securely provision keys) to identify and authenticate the device, and
    - usable (as a means to securely provision keys) to bind content to host and/or storage.

Link Control/Protection

- The platform shall have the ability to protect any HDCP protectable output with HDCP 2.2 or better.
- The platform shall secure output selection so that only authorized code can enable other outputs.

End-to-End System Best Practices

Forensic Watermarking

- The system shall have the ability to securely forensically mark video at the server and/or client to recover information necessary to address breaches.
- The watermarking shall be robust against corruption of the forensic information.

- The watermark shall be inserted on the server or on the client such that the valid insertion is guaranteed even if the device and its secrets are compromised.

Playback Control Watermark

- A compliant system shall implement Cinavia playback controls on all content.

Breach Response

- Processes and agreements shall be in place to enable rapid response in renewing any compromised software component of the system.

Certification

- The compliance of the system and the robustness of its implementation shall be certified by a combination of 3rd parties and trusted implementers.
- Necessary cryptographic elements, e.g., code signing keys, for an implementation shall not be issued until that implementation has been certified.