MovieLabs Specification for Enhanced Content Protection – Version 1.2

August 2018

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, including Ultra HD. Each studio will determine individually which practices are prerequisites to the distribution of its content in any particular situation.

Features are divided into three sections: DRM System Specifications, Platform Specifications and End-to-End System Specifications. Providers of hardware and software platforms should pay particular attention to the sections on platform and end-to-end system requirements. DRM providers need to review the sections on DRM and end-to-end system requirements.

Version 1.1 of the document updates the specification, primarily to clarify the intent of the original requirements published in September 2013.

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 problems presented 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 Specifications

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, including but not limited to timing attacks, simple power analysis (SPA), differential power analysis (DPA), simple electro-magnetic analysis (SEMA), and differential electro-magnetic analysis (DEMA), that utilize a commercially viable level of effort, e.g., number of traces. The resistance shall be established through testing, e.g., through statistical analysis of test signals for leakage.

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

- Security-related software shall be implemented in diverse ways so that an attack is unlikely to be portable. This diversity shall vary by version of the system and by platform.

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.)

Integrity & Robustness

- Runtime integrity checking of the DRM system must be performed either by the DRM system or by the platform.
- The system shall implement all mitigations for side channel attacks, including cache and timing side channel attacks, recommended by the providers of the underlying microprocessor architectures, firmware and secure operating systems.
- The system shall implement additional mitigation against cache, timing, and code injection attacks and against reverse engineering, such as obfuscation and address space layout randomization.
- The system shall use the platform isolation and trust mechanisms specified in the Platform Specification section below.

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 subsidiary code-signing certificates 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.
- The system shall proactively renew its security related software components.
- The security provider shall actively monitor for breaches.

Outputs & Link Protection

- The system shall support the requirement of HDCP 2.2 or better for specific content types, e.g., Ultra HD or enhanced HD.
- The system shall support the requirement of HDCP 2.2 or better by the content provider, e.g., in the license.
- When HDCP 2.2 is required by the content, the requirement must be enforced on downstream link protection devices, i.e., using the Type 1 flag in HDCP.
- The system shall have the ability to acquire link protection revocation lists and/or query a server to determine when compromised or non-compliant link protection devices are present and then securely limit what content can be played.
- The system shall allow other available outputs and their associated protection to be selectable by the content provider, e.g., in the license.

Platform Specifications

Encryption

- The platform shall support a content cipher of AES 128 or better.
- The platform shall provide the support necessary to make a DRM system resistant to side-channel attacks as specified in the DRM section above.
- The platform shall support a random number generator compliant with NIST 800-90C, AIS-31 or GM/T 0005-2012.

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 using the isolation and trust mechanisms described below.

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, including implementing all of the relevant mitigations for cache side channel attacks recommended by the providers of its microprocessor architecture, firmware and secure operating system.
- The platform should 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 provide a secure mechanism for DRM systems to store secrets in local, persistent storage in a form encrypted uniquely for the device and, if the platform supports multiple trusted applications or DRMs, uniquely for each in a way that securely prevents a trusted application from decrypting the secrets of others. The encryption must be rooted in a secret, immutable, device-unique value with at least 128 bits of entropy.

Link Control/Protection

- The platform shall support HDCP 2.2 or better on all HDCP protectable outputs.[1]
- Devices with HDCP protectable inputs, e.g., displays, receivers and head-mounted displays, shall support HDCP 2.2.
- The platform shall provide a secure, unforgeable means of enumerating the unique identities of all downstream link protection sink devices.
- The platform shall secure output selection so that only authorized code can enable other outputs.

End-to-End System Specifications

Link Control/Protection

- The system shall have the ability to propagate reliably the unique identities of compromised or non-compliant link protection sink devices to the source device. This propagation has to be protected in integrity and availability.
- Link protection sink components shall have unique, unforgeable, and traceable identities.

[1] Other link protection systems with hardware-based robustness rules will be considered for addition to this specification.

- Link protection sink components shall not be enabled to operate until their delivery to the manufacture of the consumer device containing them. This enabling must be controlled and secured cryptographically by the maker of the sink component.

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 watermark shall be robust against corruption of the forensic information, including collusion attacks, and transformations and capture techniques that leave the content still watchable.
- The watermark shall be inserted on the server or on the client such that the valid insertion is guaranteed during playback even if the device and its secrets are compromised.[2].

Playback Control Watermark

- A compliant system should implement Cinavia playback controls on all content. Devices in closed systems that have no access to unlicensed content are exempt from this recommendation, e.g., closed airline VOD systems.

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.
- Forensic watermarks shall be tested for robustness by a 3rd party.
- Prior to certification, the number of devices that can decrypt production titles shall be securely limited to a small number.
- Development code shall be securely prevented from running on production units, e.g., by revoking the signing certificate or by using a different root certificate and hardware root of trust.
- Production code shall limit, to the extent technically feasible, any information that could be useful to reverse engineering, such as debugging, tracing, or symbolic information.

[2] For example, insertion could be guaranteed using a cryptographically bound watermarking scheme such as that proposed in the draft MPEG-B Part 12: Sample variants in the ISO base media file format. http://kikaku.itscj.ipsj.or.jp/sc29/open/29view/29n14373t.doc

