MovieLabs Security Practices for Delivering Auxiliary Content to Devices in Cinemas – Version 1.0

August 2024

Introduction

For many, the availability of accessibility content in theaters is important to the enjoyment of the cinema experience. This includes content such as Audio Descriptions for those with visually impairments and descriptive subtitles and sign language for those with hearing impairments.

Technically, there are multiple mechanisms for delivering this content. It may be delivered in a Digital Cinema Packages (DCP) using the Digital Cinema System Standards (DCSS) and either rendered in an "open" fashion for all patrons, or in a "closed" fashion on devices for each individual patron. This DCP-based approach leverages existing security and synchronization mechanisms from DCSS, but DCSS does not cover the security of client devices.

Other approaches include delivery over the Internet to individual devices with known and approved operating systems. This approach needs to rely on other synchronization mechanisms and must also address security issues related to the preparation, distribution, and playback of the accessibility content. Alternate language content is sometimes delivered and synchronized in a similar manner. The practices in this document are intended to cover both streaming and download use cases, as well as both pre-scheduled and in-theater arrangement of playback sessions.

This document lays out some of the security issues for the delivery of accessibility and alternate language content and puts forward practices to help address them.

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.

Copyright © 2024, Motion Picture Laboratories, Inc.

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 protecting content in distribution is to mitigate piracy by reducing the quality, availability, and timing of material that is found in unlicensed distribution.

Unlicensed Distribution of A/V Tracks

The pristine digital video and audio tracks are the most important to protect. Leaks of content during the period before and during the theatrical window are especially damaging. As content providers expand the availability of accessible content onto a wider range of devices, the protection of these assets becomes even more important.

Supply Chain Leaks

Leaks of copies from the businesses preparing, distributing, and exhibiting content are especially damaging because they often occur early and consist of pristine digital copies.

Copyright © 2024, Motion Picture Laboratories, Inc.

Unlicensed Capture of Digital Files or Streams

Digital capture threats include accessing files or streams containing video or audio tracks, as well as data files such as closed captions, and decrypting them if necessary.

Unlicensed Capture of Analog Signals

Threats for the capture of analog signals include the recording of video from a movie screen, ambient sound from speakers, or an analog sound signal from a headset connector. These are difficult to prevent using current DRM techniques alone. The widespread use of mobile devices for accessibility in theaters will make it more difficult to determine whether an audience member is recording the screen.

Supply Chain

Source Tracks

- When audio tracks for the distributed work need to be processed to generate Synchronization Material (e.g., audio fingerprints) for the playback of the Auxiliary Tracks, those audio tracks should only be used to prepare that synchronization material. The generated Synchronization Material used during playback shall not be the full audio track nor in a form from which an audio track for the distributed work can be derived.
- During the preparation of Synchronization Material, any audio tracks for the distributed work that are used shall be protected according to industry best practices, e.g., those of the MPA Content Security Program[1] or of the Trusted Partner Network.[2]

Auxiliary Tracks

- Auxiliary audio, video, and text tracks shall also be protected according to industry best practices during their production and preparation for distribution.

Distribution Platform

Encryption

- Auxiliary Track content shall be encrypted using AES-128 or better prior to being downloaded or streamed to devices.

[1] https://www.motionpictures.org/wp-content/uploads/2022/02/MPA-Best-Practices-Common-Guidelines-V4.10-FINAL.pdf
[2] https://www.ttpn.org/

Copyright © 2024, Motion Picture Laboratories, Inc.

- Auxiliary tracks for different distributed works shall use different content encryption keys.
- Keys for decrypting Auxiliary Tracks shall only be distributed to authorized software running on authorized devices.

Watermarking

- Auxiliary audio and video tracks should contain a session-based watermark unique to the download or streamed session sufficient to recover information needed to address breaches, using a watermarking technology approved by the content provider.

Client Platform

Allowed Clients

- The client device application shall only be installable on iOS, iPadOS, and Android smartphones and tablets running OS versions that continue to receive security updates.[3]

Encryption

- Auxiliary Tracks shall be encrypted prior to being sent to client devices and decrypted only in memory during playback.

Acquisition & Retention

- Auxiliary Tracks and decryption keys shall not be provided to rooted or jailbroken devices.
- Auxiliary Tracks and decryption keys shall not be downloaded to the device more than 48 hours prior to the target showing or before the first day of exhibition in the licensed territory, whichever is later. They shall be deleted from the device no more than 24 hours after that showing of the movie has ended.
- The download of Auxiliary Tracks shall be limited using effective geolocation means to within a specified distance of the target showing or within the territory as required by circumstances.
- The download of Auxiliary Tracks for a title shall be limited to no more than a specified number times per account per device per showing.

Playback

- Decryption and playback shall occur only within 24 hours of the time of the target showing and no more than 24 hours after initiated.

[3] As of July 2024, this means iOS and iPadOS version 14 or higher and Android version 11 or higher.

Copyright © 2024, Motion Picture Laboratories, Inc.

- Decryption and playback shall occur only after geolocating the device to within 100 meters of the target showing.
- Decryption and playback shall occur only if synchronization material is present and usable. If the synchronization fails, the playback should continue no more than 2 minutes after the loss.

A/V Capture

- While an Auxiliary Track is being played, the device's audio and video capture capabilities shall be disabled, and incoming calls and messages should be muted.

Governance

Breach Response

- Processes and agreements shall be in place between the content provider and service providers to enable a rapid response and investigation of any leaks of content to identify any technical or process vulnerabilities.
- Processes and agreements shall be in place to enable rapid response to rectify any technical or process vulnerabilities that have been identified.
- Service Providers shall adhere to all revocation requirements agreed to with the content provider.

Security Assessments

- The security of the preparation, distribution, and playback shall be evaluated by independent security assessors, e.g., by a combination of audits of the supply chain workflow, distribution platform, and client application.

Copyright © 2024, Motion Picture Laboratories, Inc.