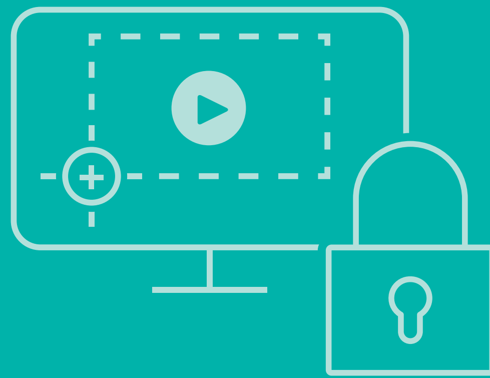
intertrust

Can Screen Capturing be Prevented?



Introduction

Screen capturing refers to the practice of recording snapshots or an entire video output on a display device. This process can circumvent copy protection mechanisms, and create illegal copies of digital content such as images and full-length movies. In some cases, the illegally captured content is redistributed to unauthorized viewers, otherwise known as restreaming piracy.

To prevent illegal screen capturing, app developers need an end-to-end solution that provides protection to block capture during playback and track restreaming piracy as well.

The protection measures provided by Intertrust ExpressPlay® binary SDKs for iOS or Android on native applications protect these platforms. Content protection can also be enforced using ExpressPlay Multi-DRM Service to deliver Apple Fairplay Streaming, Microsoft PlayReady, or Google Widevine DRM licenses to native clients or web applications.

Application developers use modern content protection solutions such as ExpressPlay DRM to address stringent studio requirements for licensing HD and Ultra HD content.

This includes:

- Preventing screen capturing
- Preventing re-transmission of the video (through mirroring or casting)
- Engaging high-bandwidth digital content protection (HDCP) on digital outputs, or disabling digital outputs when HDCP cannot be enforced

Software measures to prevent screen capturing

Both iOS and Android offer software-based mechanisms to prevent the user display from being recorded.

On iOS, AirPlay Mirroring is enabled by default and it is possible to disable it programmatically from within an app through the dedicated API exposed by the iOS SDK (5.0 or later), for example, by setting the properties such as allowsExternalPlayback to false.

Moreover, with iOS it is not possible to control an HDMI output from enforcing HDCP. In addition, it is not possible to control which screen content is rendered on. As a consequence, if HDCP needs to be enforced for specific content, the recommendation is that the application prevents playback of DRM-protected content when an external screen is attached to the device. Also in this case, it is possible to programmatically detect within the app whether an external display has been connected to the iOS device and if so, to prevent or stop the playback.

It should be noted that iOS 11 offers a screen recording feature, which lets a user record the screen locally. However, the iOS SDK also provides a set of native APIs that allow an app to detect when screen recording is taking place. This allows applications to act accordingly, for instance, to prevent recording when protected content is being played.

Android devices behave slightly differently compared to iOS. Since Android API Level 17 (Android 4.2), Google introduced the ability to control and secure the "surface," or the built-in display, where the content is rendered. This means that the content can neither be captured nor rendered on a non-secure display (even when mirrored). These Android APIs are guaranteed to effectively function only if the device supports Widevine DRM, although the content itself does not need DRM-protection for the app to benefit from this functionality.

Android "rooting" tools, and the iOS equivalents for "jailbreaking" devices, are available and permit bypassing any screen capture prevention or output control. On the other hand, when the ExpressPlay binary SDK is used, it allows the detection whether or not an app runs on a rooted device.

Screen capturing and DRM

When using ExpressPlay Multi-DRM service to deliver Apple FPS DRM or Google Widevine DRM licenses to native applications or web applications, the device will automatically enforce that the video portion of the protected content on Safari and Chrome cannot be captured or recorded.

[1]'Jailbreaking' and 'rooting' denote methods of bypassing or replacing software originally installed by device designers and carriers, and are more often than not associated with piracy.

Desktop HTML5 applications

In modern browsers supporting HTML5 Encrypted Media Extensions (EME)/Media Source Extensions (MSE), the DRM is integrated through a Content Decryption Module (CDM) component integrated with the browser. Browsers usually support a single DRM scheme in their implementation, depending on the browser OS.

The table below provides a summary of the major platforms and browsers, and it also highlights the integration level of the DRM (through the CDM) and the ability to record premium content via screen capturing methods.

Platform	Windows 10			Mac OS	
Browser	Edge	IE11	Chrome/ Firefox	Safari	Chrome/ Firefox

DRM	PlayReady	Widevine	FairPlay
DRM Integration Level	Platform	Software	Platform
Screen Capture/ Screen Recording	Prevented	Possible	Prevented

While screen capturing cannot be eliminated completely, comprehensive content protection and compliance are possible with Intertrust ExpressPlay. To learn more, please visit **intertrust.com/products/drm-system/**

intertrust®

Building trust for
the connected world.

Learn more at: intertrust.com/drm
Contact us at: +1 415 209 5057

Intertrust Technologies Corporation
920 Stewart Drive, Sunnyvale, CA 94085