5 HOW TO TRUST ▷ YOUR PLAYER

Presented by BITMOVIN Friend MTS intertrust

BUILDING AN OTT SERVICE FOR TODAY'S WORLD

Article 5 – From One End to the Other: Protecting Content From Origination to Playback, Once and for All

Published Date: November 12, 2020

Joshua Shulman, Digital Marketing Specialist, Bitmovin
Alan Ogilvie, Lead Product Manager, Friend MTS
Ali Hodjat, Product Marketing Director, Intertrust Technologies

Any player in the OTT world would have a hard time keeping up with the myriad of changes we have seen over the past several months: COVID-19. The dramatic increase in video consumption. The exponential rise in subscriptions to established OTT streaming services. New OTT streaming services. PVOD. Fragmentation of content. But enter the other player – the content pirate – and things become even more complicated.

As we reviewed in our **first article**, the stakes are high – very high. A recent report from **Parks Associates** finds that the value of pirate video services accessed by pay-TV and non-pay TV consumers will exceed $67 billion (USD) worldwide by 2023. Another report from **ABI Research** estimates that more than 17% of worldwide video streaming users access content illegally. The impact on OTT streaming services is a direct and significant blow to the bottom line.

Securing OTT Content

To stay alive in this environment, OTT companies have no choice but to secure content delivery and playback at a multiplayer level, which includes:

- Protecting content with technology *within and around* the video player: the consumer playback experience.
- Protecting content *from* "players": the pirates – the potential bad actors looking to compromise your service, and steal content. This is the human factor.

If you're an OTT service launching premium exclusive content, don't be the one that suddenly discovers your content appearing, and then being distributed through pirate services, within minutes of launch.

Digital Rights Management (DRM)

Often considered the cornerstone of content and revenue protection strategy, **digital rights management (DRM)** remains a critical part of an effective multi-prong system. In **Article 2**, **Intertrust Technologies** discussed the pros and cons of two DRM license acquisition models (direct acquisition model, from a license server, and proxy license acquisition model, from a proxy server).

Intertrust also discussed DRM best practices for leveraging a cloud-based DRM service to protect high-value streaming content. OTT operators must follow these to block the loopholes that hackers otherwise may use to defeat the purpose of DRM technology.

- **Multiple content encryption keys (CEK)** – Setting different CEKs for audio track, as well as for each video resolution, enables OTT streaming service providers to grant access to content distributed to different customers/different devices. They can do this by delivering only the DRM licenses with CEKs for the authorized resolutions based on the consumer's subscription package.
- **DRM security levels** – Defining the security tier of the DRM stack that is supported by the target device, with two relevant distinctions: software-based DRM client and hardware-based DRM client. Using the right DRM security level allows OTT streaming service providers to map the required security level for each given resolution or track.
- **Widevine Verified Media Path (VMP)** – The requirement enforced by Google Widevine DRM is specifically relevant when a browser-based video player is used to decrypt Widevine-protected content. Given Google's recent policy to strictly enforce the VMP requirement, Widevine license servers can only issue licenses for content decryption modules that support the VMP feature.

Securing the Playback Experience

Delivering high-value premium content to a web browser can be a risky venture, but one that is critical to reaching audiences today. Browser environments are amongst the farthest-reaching, but least secure, due to their open nature, and require some extra attention when implementing content protection systems.

Bitmovin highlighted in **Article 3** how code obfuscation tools and techniques work in browser playback environments where website code (JavaScript) is interpreted and executed. The result is code that is extremely difficult to read and reverse-engineer, either by tinkerers or a more determined actor…such as a content pirate.

Yet executing code on a web browser, following open JavaScript standards, remains impossible to completely secure playback. Someone with enough motivation, and time to spend gathering intelligence and doing research, will eventually be able to reverse-engineer your playback code. In reviewing its web player, Bitmovin detailed how concurrent management and domain locking work as part of a complete defense strategy to deter attacks from content pirates.

Finally, once an OTT provider has secured its **distribution chain from source to the playback environment**, and has followed best practices to secure the playback experience as much as possible, Bitmovin summarized three golden rules to boost users' experience – and ultimately, your brand.

Watermarking and Monitoring

For all of its merits, the reality is that DRM only protects the delivery and distribution of content to the point of consumption. In **Article 4**, **Friend MTS** showed that beyond DRM there is a need to detect pirated content, deter wrongdoers by identifying them in stolen content, and take action to stop further loss of revenue by disabling access to the service.

Although DRM protects the content until it arrives at its intended legitimate destination, additional precautions should be made to stop content from being redistributed by those who have no rights to do so.

Commonly pirates will capture content directly from the screen (with the use of screen recording software) or a device's digital output with rights management removed. They're able to rip the stream once the content is decrypted by the authorized devices.

So, if DRM protects only the legitimate path from origination to the point of consumption, the OTT operator must protect the value of video content – whether original or rights-managed – outside of these service boundaries. **How?** Forensic subscriber-level watermarking can be employed on any delivered video in the service. Doing so affords the ability to identify the 'subscriber', your legitimate user. Using a combination of active monitoring of piracy groups and sites – suspected pirate materials are identified through known reference fingerprints, and an extraction process can take place to obtain the subscriber identifying data within the watermark. This can rapidly signpost the "bad actors", low volume content sharers, and industrial-scale pirates. Action can then be taken to stop the content from being accessed and used for piracy.

With an effective subscriber-level watermarking solution, you can close the loop and start to lock down piracy at its source.

Friend MTS reviewed the pros and cons of A/B variant (server-side) and client-composited (server-side + client-side) watermarking in an OTT environment and looked at how they are deployed and function. Client-composited is the clear winner with its rapid detection of content theft, lower overall cost, reduced deployment complexity, faster time-to-market, and higher adaptability to attacks on watermarks.

In looking at the characteristics of an effective client-composited watermarking service, Friend MTS outlined its Advanced Subscriber Identification (**ASiD**) service, which has retained its agility to fend off attacks and has proven robustness in both broadcast and OTT environments. They highlighted the importance of a watermarking provider not only keeping up with the latest pirate schemes but staying ahead of them. They also detailed the key watermarking features of speed, global reach and ability to deliver through a multi-CDN service – all within the context of live sports and entertainment, pay-per-view and on-demand content.

Article 4 also highlights the need to understand the 'human factor' in your OTT service – the end-users who are consuming content. Friend MTS advised starting with a position of 'zero trust' for your users – assume some users of your service will attempt to circumvent security controls or use your service in a way you didn't intend. Errant or undesired behavior within your service can be broken down into various 'personas' and the article takes you through several of these.

Once user behaviours are understood, you can plan your monitoring architecture, and how your business support systems should respond to service misuse.

Conclusion

Today's OTT world is radically different than it was in early 2020. Bad actors abound. Content and revenue are at risk literally every minute of every day around the world. But you do not need to be a victim.

It's possible to take steps upfront to secure content, working with a multi-pronged strategy that integrates DRM, forensic watermarking, player security, and robust monitoring to produce a real solution to the problem of content piracy. In today's world, "end-to-end" is not just an IT buzzword. It's a way of delivering streaming media to a playback client in the most secure and protective environment that we can achieve.

To learn more about "How to Trust Your Player," check out the other articles in our series:

- **Article 1 – Tips from the Top: Secure Content Delivery and Playback**
- **Article 2 – Securing Content Access with Digital Rights Management Best Practices**
- **Article 3 – Tips and Tricks: How to Secure Your Content in Challenging Streaming Environments**
- **Article 4 – Beyond Digital Rights Management: Video Watermarking Weighs In**
- **Article 5 – From One End to the Other: Protecting Content From Origination to Playback, Once and for All**

Still want to learn more? View our associated Fireside Chat sessions:

- **Video 1 – Tips from the Top: Secure Content Delivery and Playback**
- **Video 2 – Securing Content Access with Digital Rights Management Best Practices**
- **Video 3 – Tips and Tricks: How to Secure Your Content in Challenging Streaming Environments**
- **Video 4 – Beyond Digital Rights Management: Video Watermarking Weighs In**

Check out the recording of our How To Trust Your Player Webinar: **View Recording**.

For information on redistributing this content, please reach out to **pr@friendmts.com**.

How To Trust Your Player is a collaborative effort between Bitmovin, Friend MTS and Intertrust. Our goal is to educate media and content providers on the importance of delivering streaming content in the most secure ways possible from the video player to the end-consumer while protecting both their content and revenue.

Bitmovin

Bitmovin is a developer of video streaming technology. Built for technical professionals in the OTT video market, the company's software solutions work to provide the best viewer experience imaginable by optimizing customer operations and reducing time to market.

Bitmovin's solution suite – a video encoder, player, and analytics platform – lets content owners redefine the viewer experience through API-based workflow optimization, fast content turnaround, and scalability.

Founded in 2012, the company is based in San Francisco, with offices in major cities in Europe, North America and South America. With more than 250 enterprise customers around the globe, Bitmovin helps power clients like BBC, fuboTV, Hulu Japan, RTL, and iFlix.

Friend MTS

Friend MTS helps media and entertainment businesses secure content so that revenue can grow and creativity can thrive.

With advanced services that measure, monitor, detect and disable content piracy, Friend MTS provides a 360-degree
view of the constantly shifting content piracy protection ecosystem and stays a step ahead of ever-advancing and sophisticated content piracy behavior and technology with a sharp, deliberate, laser-focused commitment to continual monitoring and innovation.

Businesses and nonprofit organizations throughout the world recognize Friend MTS as the leading authority for content and revenue protection. The company also has donated its digital fingerprint technology to the International Center for Missing and Exploited Children to tackle child abuse content online.

Founded in 2000, Friend MTS is headquartered in Birmingham, England, with operations throughout Europe, the Middle East, Africa, Latin America, and North America. Friend MTS is the recipient of an Emmy® Award for Technology and Engineering, presented by the National Academy of Television Arts and Sciences (2018).

Intertrust Technologies

Intertrust provides the world's leading digital rights management (DRM) cloud service with a complete ecosystem of security and rights management products. We empower businesses to securely manage all of their data and devices, regardless of location, format, or type–enabling innovative multi-party apps and services.

Intertrust Media Solutions provides robust content protection solutions for Media and Entertainment. Intertrust ExpressPlay consists of a cloud-based multi-DRM service, broadcast TV security and anti-piracy services with proven scalability in the largest OTT streaming platforms globally.

ExpressPlay DRM™ is today's most complete multi-DRM monetization service for OTT streaming supporting Apple FairPlay Streaming, Google Widevine, Microsoft PlayReady, Adobe Primetime, and the open-standard Marlin DRM. Intertrust also offers ExpressPlay DRM Offline to enable secure streaming of premium content through an offline multi-DRM platform.

Founded in 1990, Intertrust is headquartered in Sunnyvale, California, with regional offices in London, Tokyo, Mumbai, Bangalore, Beijing, Seoul, Riga, and Tallinn.