Beyond DRM: The Complete Content Protection Story

Written by Steven Hawley

The scale and complexity of the contemporary piracy landscape should not be underestimated. This three-part series of articles explains why it is not enough to implement a digital rights management (DRM) system and what solutions need to be in place for complete premium video content protection to prevent its illegal redistribution.

TABLE OF CONTENTS

BEYOND DRM PART 1

1 Fighting content piracy and illegal restreaming—Why DRM is not enough

Piracy is a huge business. The U.S. Department of Commerce estimated[1] that the U.S. economy suffers at least $29.2 billion in revenue losses each year. By 2023, the revenue to pirates of pay TV and non-pay TV video may exceed $67 billion worldwide, according to a 2020 forecast published by Parks Associates.[2]

Video pirates have become the biggest source of competition against pay TV and premium streaming services. Parks estimates that the U.S. pay TV industry would lose about a billion dollars if just 10% of pay TV subscribers quit pay TV in favor of pirate services.

Today's video pirates have high production values and offer good video quality, sometimes tricking consumers into thinking that they are legitimate. The appeal of a source with hundreds or thousands of video sources for one low price for all of your devices is compelling.

The value of today's video content

It's a fact of the video industry that content continues to grow ever more valuable and there are many examples to support that claim. Premium television programming developed for pay TV and streamed direct-to-consumer via TV Everywhere and OTT service models. Ultra HD programming, for which video providers can charge a premium in some situations. Premium live league sports programming such as the English Premier League and WWE. Early window movies via video-on-demand. Not to mention emerging experiences like multi-angle, immersive and 360° viewing.

As quality and value continue to increase, it's more important than ever to protect against theft and infringing use. Once the programming has been lost to piracy, its value is seriously compromised. One famous sports broadcaster has remarked that piracy has made its exclusivity agreements with the sports leagues essentially meaningless.[3]

Traditional countermeasures are effective, but only to a point

Digital rights management (DRM) has long been a basic component of audio and video service delivery via the open Internet, to secure it against infringing use; by Internet service providers, content providers

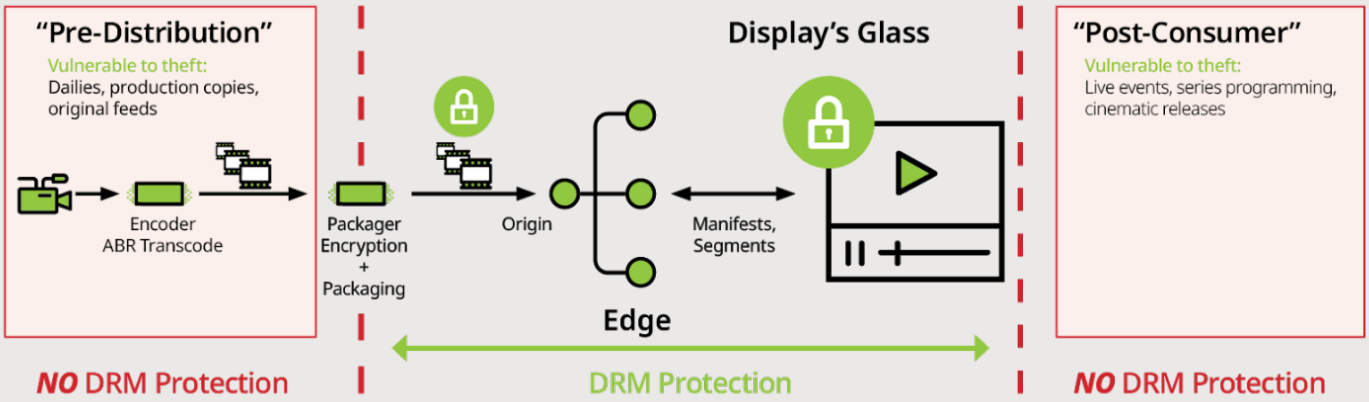

Figure 1: How DRM protects only the legitimate service domain
Source: Friend MTS

and with pay TV services. Together, conditional access (CA) and DRM are used to enable pay TV providers to protect the services delivered as MPEG transport streams to conventional set-top boxes, and as IP-streaming services to every other screen, respectively. Broadcasters have also embraced DRM, as they take their own services online.

DRM has its advantages. Unlike CA, which protects services only within the context of a pay TV operator's managed distribution framework, DRM protects content delivery even when it is made available outside of that delivery network, such as via the open Internet.

But CA and DRM are effective only up to the point of consumption.

What happens when the content 'escapes'?

When the consumer requests a streaming session, the user is authenticated, and a license is issued by the DRM system to enable the content to be viewed on the consumer's device.

Once the DRM protection is lifted and content is in the clear, there's risk that recipients may capture it and profit by re-distributing it outside of its legitimate intent, beyond the outermost point of legitimate consumption. This is the **post-consumer** world for the content.

Pirates obtain content through HDMI-ripping, video capture from a player or screen-scraping session, by linking to video streams or downloads that are hosted by other pirates, or from legitimate streams that were inadequately secured in the first place.

What happens to stolen content?

Pirates use a variety of illegal distribution models. One of them is hosted wholesale distribution, which caters to streaming sites that act as resellers by linking between the hosted content and consumer-facing websites. Another is hosting of content in online cyberlockers.

Pirates also commission illicit streaming devices (ISDs), sold online and in physical retail outlets, that are pre-programmed to access pirate app stores and stolen content.

The distribution itself is via streaming, downloads, torrents, and P2P streaming, to destinations that include web browsers and apps running on legitimate personal computers, mobile devices, streaming video and hybrid-IP set-top boxes. Pirated offerings are promoted through social media, advertising and by word of mouth.

How can piracy be stopped?

It's easy to see how valuable video content can be stolen and redistributed in a variety of ways even with CA/DRM present in the delivery chain. Now, how do we stop it? Before an instance of piracy can be stopped, the stolen content has to be identified as having been stolen, and the theft needs to be verified back to its outermost / last legitimate source.

References

1. David Blackburn, PhD., Jeffrey A. Eisenach, PhD., David Harrison Jr., PhD. *Impacts of Digital Video Piracy on the U.S. Economy.* June, 2019. Research report. NERA Economic Consulting for Global Innovation Policy Center, United States Department of Commerce. See: theglobalipcenter.com
2. Steven Hawley. *Video Piracy: Ecosystem, Risks and Impact.* January, 2020. Research report. Parks Associates. See: parksassociates.com
3. This is reference to a comment made by beIN Media CEO Yousef al-Baidly at an October 2019 event in London. See: piracymonitor.org

See page four, *for an examination of the types of technology solutions required to address illegal re-distribution, with a focus on watermarking and establish the most effective approaches for securing your content.*

BEYOND DRM PART 2

2 Beyond DRM: Completing the content protection story

In Part 1, we recognized video piracy as an expensive risk for video providers, and showed that once the content has arrived at its intended legitimate destination, the traditional video security techniques of Conditional Access and DRM can do nothing to stop it from being redistributed by entities that have no rights to do so. The security shortcoming stems from the fact that only the legitimate path from origination to the point of consumption is being secured.

Credential management as an access management tool

Today's video services are protected by a 'front door' that challenges the consumer to provide access credentials in the form of a user ID and a password, before being admitted to access the service.

In the days of traditional set-top boxes, before streaming services, credential sharing outside the home was relatively pointless for legitimate access. You had to be in the home, in the presence of a set-top box that was paired with the credentials, in order to gain access. But with streaming, where the consumer can be anywhere, credential abuse has become commonplace.

Password sharing, and consumer video account abuse have captured the video industry's attention in recent months and years, but, like DRM, the management of credential abuse and credential theft don't help reduce the distribution of content once it has escaped the boundaries of a video service.

Identifying video content that has been discovered out-of-bounds

To protect the value of premium video content outside of these legitimate service boundaries, the video itself needs to be identified in a way that confirms its outermost point of legitimate use. Once that is known, infringing users and industrial-scale pirates can be identified.

To fill these gaps in protection not covered by DRM or CA, video providers can embed information into the video payload itself, which can occur at the

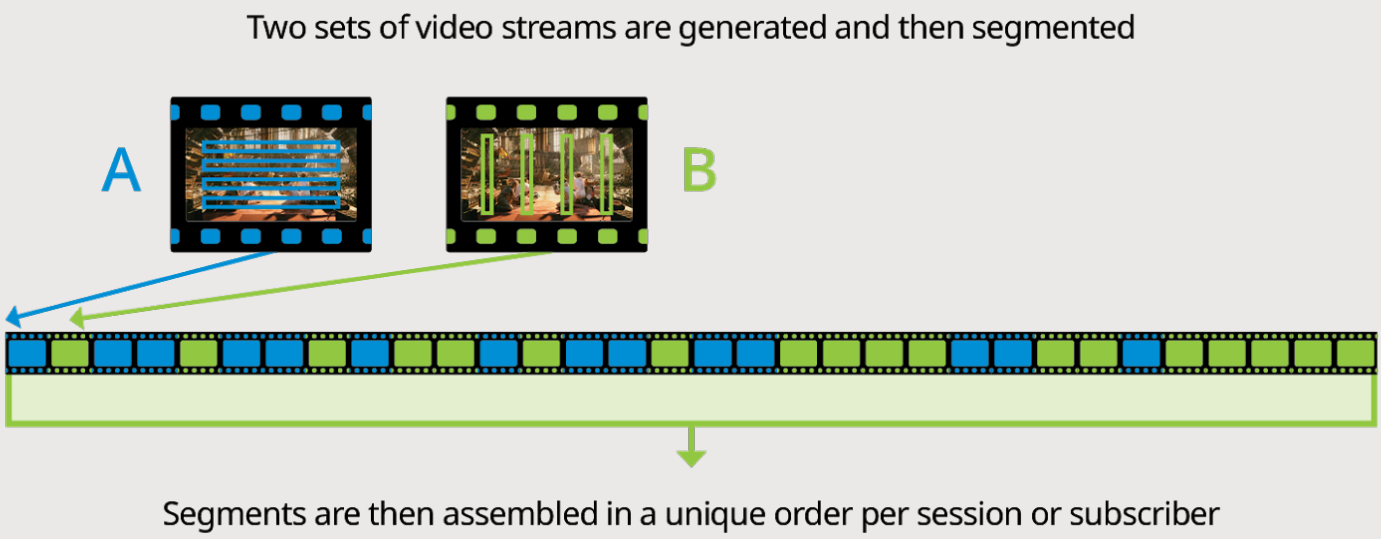

Figure 1: Combining two sets of watermarked video
Source: Friend MTS. Image source: frames from (CC) Blender Foundation | mango.blender.org

origin, in the CDN during distribution or within the player device. Forensic watermarking has emerged as a preferred technique.

Payload information contained within the watermark can include the device IP address, session details, subscriber identifier, or other information.

While consumers can't see the watermarks, automated analysis can. Let's look at two watermarking methods that are common for IP streaming.

About server-side, or A/B variant watermarking

One technique, called A/B variant watermarking, is performed within the service provider's facilities, "upstream" from the ultimate consumer at the video provider's headend, or in the distribution network.

A/B variant replicates every streaming session into "A" and "B" streams, each of which receives a different watermark *(Figure 1)*. These streams are then broken up into segments which are then combined into a single stream containing a unique combination of A and B segments so that no two users receive the same sequence.

Due to this dual stream approach, A/B variant watermarking is resource-intensive, and therefore costly, at the OTT headend. Each video source (every live video channel, for example) must be encoded twice and distributed simultaneously, meaning that the video provider needs two sets of encoders, and sufficient storage and origination resources to accommodate the two sets of streams.

There are certain additional security steps that are needed when implementing A/B variant watermarking. One is to ensure that the A and B segments can't be discerned when they are received for playback. Another is protecting A/B variant watermarking from several forms of man-in-the-middle attacks. There are also challenges with how A/B variant watermarking would work in low latency live streaming situations.

In summary, A/B variant watermarking requires additional resource in the OTT headend, with associated costs, and security enhancements to increase its robustness, including against man-in-the-middle attacks.

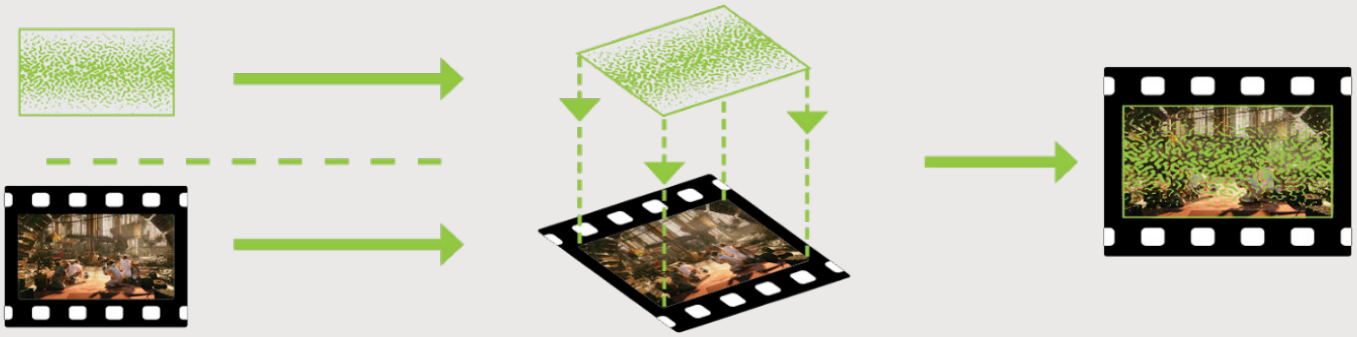

Figure 2: Watermark is composited with the video frame
Source: Friend MTS.

About client-composited watermarking

An alternative to A/B variant watermarking is client-composited watermarking, where the watermarking process occurs within the consumer device. The embedded player implements a software library that is used to access a database that replies with a unique identifier. The watermark payload is converted into a pattern, similar in concept to a QR code, and then composited over the video *(Figure 2)*.

The client-composited watermarking approach has multiple benefits that make it preferable to the A/B variant approach in certain situations.

One benefit is the time to detection, which can be as little as a few seconds.

In A/B variant watermarking of HLS-encoded adaptive bit-rate streams, using six-second segments, the amount of time necessary to cycle through the segments and positively identify the session could take as much as seven minutes. If segments were two seconds long, it's still about 2 ½ minutes. This makes the A/B variant approach less effective for live sporting events where a match or a race could be over by the time the infringing user has been identified.

Another benefit is low cost.

Unlike A/B variant watermarking, there is no need to implement two sets of video processing, storage, and origination resources. Another benefit of client-composited watermarking is that the watermark generation and compositing processes use client-side software and don't require any hardware modifications at the OTT headend.

And finally, this process works equally well with live and on-demand services as there is no added latency which, in the case with A/B variant implementations, needs to be mitigated.

So far, we've talked about how DRM falls short in fully protecting video content. We've also identified video watermarking as a way to fill these gaps, justifying client-composited watermarking as a preferred approach. In Part 3, we'll talk about how the source of infringing use can be identified and managed.

Continue to Part 3, *the concluding article explains how to use monitoring to find watermarked (and fingerprinted) content and suggests countermeasures video providers can take against piracy.*

BEYOND DRM PART 3

3 Beyond DRM: Finding stolen content and addressing piracy

Digital rights management isn't enough to stop the redistribution of stolen video content outside of its legitimate service context. In our previous article, we described how unique but invisible identifiers can be embedded within the video. But the equation is incomplete unless there also is a way to find stolen video, identify its source, and take effective action.

Detection: Finding the needle in the haystack

Embedding watermarks alone is only half of the detection story. To make watermarking effective, stolen video must be located, which is done by monitoring suspected pirate video outlets. Detection is assisted by matching the fingerprint of a suspected asset with a reference fingerprint that was generated during the production process.

Once the suspected item has been recognized, it is analyzed to detect the presence of an identifying watermark, and then evaluated to read the information that it contains. This process is called 'extraction' or 'recovery.'

How pirates interfere with detection

Thieves don't want to be detected. To reduce the likelihood that an instance of stolen content could be traced back to its last legitimate distribution end-point or to the pirates themselves, pirates may attempt to make the watermark unreadable by applying transformations to the content.

Such transformations are called 'attacks.' A watermark that has been successfully attacked is no longer available or readable, making identification difficult or impossible.

Types of attacks include:

- Visual quality attacks such as blurring, sharpening, or changes to contrast
- Geometric transformations such as rotation, pin-cushion distortion, and mirroring
- Cropping, upscaling/downscaling, changes to aspect ratio
- Collusion attacks, where multiple instances of a video—such as outputs from multiple set-top boxes or streaming devices—are combined: example blending, interleaving, mosaicing, etc.

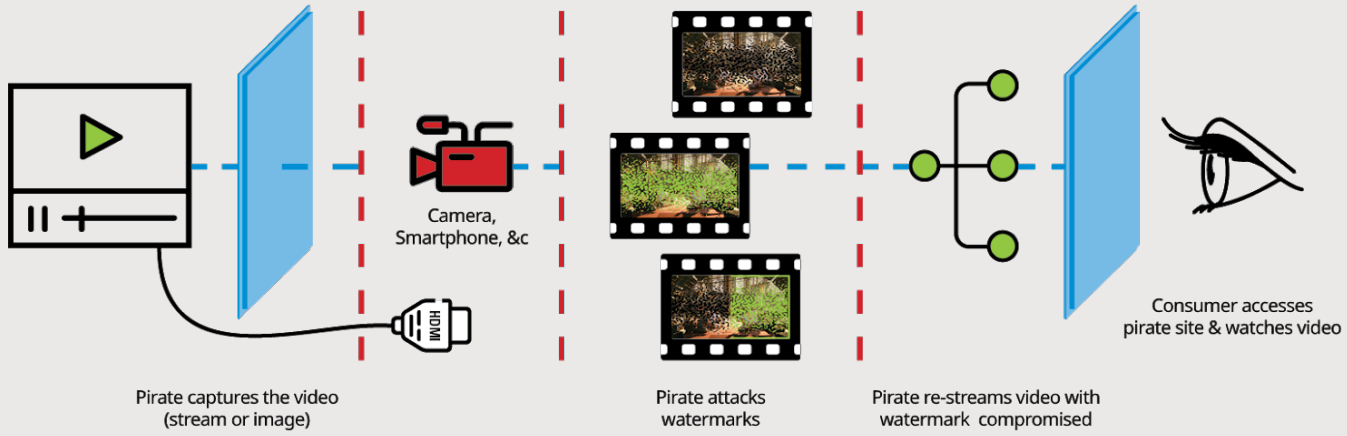

Figure 1: A pirate captures legitimate video, attacks the watermark and then re-streams it to the consumer
Source: Friend MTS.

- Format transcoding, digital-to-analog transformation
- Attacks on the delivery of the watermark itself, such as temporal disruption through streaming segment switching, or by video output switching/splicing

The diagram above shows a pirate's watermark removal workflow.

On the left side of the diagram, a pirate captures video programming using a consumer device such as a camera or smartphone, intercepting it at the HDMI connector, via screen-scraping, or by capturing the output of a player in a consumer device. The pirate then attacks the video using one or more of the methods we listed above, in an attempt to remove the watermark; and then makes the video available for re-streaming or download.

A "robust" watermarking solution has a better likelihood of surviving real-world attacks by remaining readable.

Taking action

Once the identity of an illicit video stream has been confirmed using video fingerprinting, what happens next? A decision must be made as to how to treat the incident.

A range of remedial actions are available, including direct actions against the pirate and actions against the consumer. Remediation policies themselves are either the domain of the video content's owner or license holder, the video distributor, or both.

In turn, these policies are subject to the constraints of locally-applicable regulation. In some jurisdictions, the act of consumption, in itself, is considered to be an act of piracy.

Types of actions that can be taken directly against the pirate include:

- Issue take-down notices to the pirate streaming services and escalate to their infrastructure suppliers, such as CDNs and hosting providers
- Apply for search engine link removal
- Enforce existing blocking orders
- Report to law enforcement

Most video providers are likely to take actions against subscribers whose accounts are detected to be restreaming. This can include interrupting the session or requiring the user to re-enter access credentials. Other approaches can include suspending the end user's account, disallowing the use of the device on the account, or initiating legal action. Note however that some subscribers may be unaware that their accounts have been compromised and being used to illegally restream.

Diligent monitoring of subscriber account behaviour may also identify out-of-profile usage such as increased concurrent stream usage, abnormal geographic dispersion, massive numbers of stream requests, or the use of the same financial accounts to purchase multiple streaming accounts.

Key take-aways

Anti-piracy is secretive by nature. Video providers are very careful about disclosing their methods in public forums. They don't want to reveal anti-piracy "sources and methods." They want to quietly encourage the use of their legal services

A rigorous approach to piracy detection should be part of a broader antipiracy initiative that helps maintain the market value of the premium content. But it's not just about the content. Video providers invest heavily in placing and maintaining their delivery infrastructure of systems, software, operations and technical support. Anti-piracy helps operators preserve the value of this infrastructure investment.

Risks of doing nothing

The risks of doing nothing about infringement and piracy are mixed.

On one hand, with the increasing value of content, distributed anywhere, anytime, to any device over the Internet, the risk of loss to theft and the need to minimize it have grown almost exponentially. If content is to retain its value in this environment, it's more important than ever to identify where it came from, where it is going, and to make deliberate decisions as to whether it's going where it's intended to go.

By the same token, doing nothing can reduce the risk of alienating consumers. With anti-piracy, knowing the location and disposition of video content should not necessarily be a call to action. Much can be learned by observing what happens with instances of infringement. For example, new market opportunities can be uncovered if content is found to be popular in territories where it has not been licensed.

In this light, every situation has its nuances, but it's always best to be informed. Watermarking and monitoring are important tools in that pursuit.

Download

Attacks on Subscriber Watermarking Technologies Quick Facts

Learn about the key differences between various watermarking technologies and why Client-Composited solution is the most widely used watermarking today.

Request

Attacks on Subscriber Watermarking Technologies White Paper

Based on the technical data obtained through operating the world's most extensive automated monitoring of a wide spectrum of illicit content services, Friend MTS presents a review and analysis of real-world piracy attacks aimed at circumventing watermarking content protection. Complete the form at the above link to receive the white paper.

About the author
Steven Hawley
Founder & Managing Director
Piracy Monitor
Diagrams sourced through Friend MTS

Friend MTS

Contact us for more information

Alan Ogilvie
Lead Product Manager
aogilvie@friendmts.com

Brad Parobek
Senior Vice President, Sales Americas
bparobek@friendmts.com

Simon Hanna
Regional Vice President, EMEA
shanna@friendmts.com


friendmts.com