DRM + Watermarking: Working Hand in Hand to Protect Against Piracy

Jonathan Friend
CEO, Friend MTS

It is for good reason that video services like Netflix, Hulu, Google Play Movies and Amazon Prime Video don't allow some smartphones[1] to stream movies or TV shows at higher resolutions. Digital rights management (DRM) is built into many devices and protects these services with this lockout in order to discourage piracy of these video files from illegal download and redistribution. For those media companies operating in the online streaming space, the Google-owned DRM system Widevine Level 3 (L3) is a well-known commodity in the battle against content theft. However, regardless of the level, Widewine just as any other DRM is not effective when used on its own. Watermarking technology along with piracy monitoring must go hand-in-hand with DRM, all working together to provide complete protection.

L3 is Widevine's least secure security level. Used in many devices playing back media the L3 security executes in software, not hardware, making it reversible and bypassable. For example, by hijacking calls in web browsers' Encrypted Media Extensions (EME) Widevine's content keys can be decrypted and streams using L3 can play back incredibly easily.

Obviously Friend MTS doesn't provide DRM solutions for customers, but we do care passionately that DRM is a key component of a service's anti-piracy solution. You shouldn't do subscriber-level watermarking until you have DRM robustly in place. Also DRM is not a 'set and forget'—so you have to continually review your anti-piracy solution as pirates adapt. For example: security advisories from DRM providers need to be taken seriously and action must be taken in a timely manner.

Varying from the industry response

This vulnerability that allows media encryption keys to be disclosed has prompted an interesting and entirely expected response from many: that the solution is not in trusting the client device, but in adding server-side, edge-switched subscriber watermarking.

As CEO of the company that's behind the world's most deployed and actively used subscriber watermarking system, one would expect my company to join the bandwagon in promoting the technology in a moment of limelight. After all, our watermarking is active daily in millions of devices and we perform millions of extractions a month for companies worldwide.

---

[1] *devices known to have root compromises.*

However, Friend MTS takes a fundamentally different approach to content protection, in that we are as focused as much on the outcome as we are on the technology to achieve it. It's not enough for us to make snazzy sales pitches about how our smarts and our tech alone are the solution to all your piracy woes.

Applying chess strategy to content protection

Instead, we delve inside and find out what's really going on. In fighting content theft, much like playing the game of chess, we seek to understand not just what pirates are doing right now, but what their next move will be, and the move after that.

So, rather than immediately react to this disclosure by trying to convince prospects that we have the goose that laid the golden egg, and revel in a short-term gain, we're looking at it differently. We're using this opportunity to remind everyone that expecting watermarking alone to provide any semblance of security without properly securing the media transmission with a sound implementation of DRM is a foolish notion. What's needed is an up front strategy to secure content, that integrates DRM, watermarking/monitoring and player security to produce a real solution to the problem of content piracy as we have recently discussed in How To Trust Your Player conversations with our partners.

DRM and watermarking—and indeed all security technologies—are complex systems that from time to time will be subject to successful attacks. The iterative 'cat and mouse' nature of circumventing circumvention is inherent in all security. While safety nets are a useful backup, one needs to be circumspect about the robustness of that net and carefully evaluate how much safety it actually provides.

Watermarking and DRM set out to solve fundamentally different problems, but they're nevertheless very interconnected. DRM's goal is to ensure that playback is possible only by authorised/legitimate customers, on legitimate playback devices and/or in legitimate playback software. Watermarking protects from that point onwards, where content thieves take content from a legitimate player by whatever means, and retransmit it into unauthorised (aka pirate) services.

Working hand in hand: DRM and Watermarking

Yes, as much as one might think that DRM prevents unauthorised capture/retransmission, it's also unrealistic to expect that watermarking will in any way protect the playback. Further, one is sorely wrong in expecting that watermarking will continue to provide protection if the DRM is compromised. The two systems must work together to provide complete protection, and the failure of either one will let the other side down.

Those setting out to steal your content are sophisticated and skilful. They can and will analyse and identify weaknesses in security schemes. As logical and elegant as a technology, technique or system may seem, it's critical to ask about where that technology, technique or system is and has been deployed, how it has held up against real-world attacks, and what adaptations have taken place to maintain security through recent phases.

One needs to understand that there's no such thing as an attack-proof security system. The mark of an expert in content protection is as much in how they react when the inevitable happens as in the design of their product in the first place.

So, as attractive as claims about substitution watermarking may be, with far-reaching claims about working to protect against piracy even with unmodified players/devices or compromised DRM systems, stop for a moment and think. If you're serious about the security of your content, and your revenue, take a step back and investigate further. As much as I would love to shout from the rooftops about how the world needs our technology, the reality is that you need watermarking and monitoring to be working together with DRM to provide the safety that you require.