intertrust®

White Paper

ExpressPlay

The new perspective on securing eSports

Part 2

The cost-effective path to meeting all eSports security requirements

Contents

Introduction 2

Basic requirements in eSports content protection 3
DRM systems for high-value streaming services 4
The multi-DRM mandate 4

The content protection solution eSports providers need 5
Market-leading functionality at minimum costs 5
Extensive optimization of protection for live-streamed eSports 6

Essential support for monitoring content theft & combating piracy 7
A comprehensive approach to monitoring content theft 8
Watermarking optimized for live-streaming environments 8

Mitigating eSports app vulnerabilities to malicious disruptions 9
Executing obfuscation 10
Anti-tampering protections 10
Protection against attacks on cryptographic operations 10

Conclusion 11
Footnotes 11

Introduction

The surging eSports content market is driving unprecedented growth, but also new levels of piracy and content theft, as illuminated in part 1 of this white paper series. The stakes are high, with a huge amount of revenue on the line.

After looking at the scale and sophistication of threats against eSports business operations, it can seem overwhelming to know how to respond. However, there are cost-effective ways to mitigate all these modes of attacks, as demonstrated in live-streaming operations worldwide. The main question is, what can eSports producers and distributors do to mitigate them within stringent budgetary and staffing limitations?

The answer is clear. As evidenced by the protective actions taken by a growing contingent of live streaming service providers worldwide, the cloud-based security solutions provided by ExpressPlay Media Security Suite offer the most comprehensive and cost-effective approaches both to combatting content theft and to thwarting hackers' attempts to disrupt businesses through piracy.

To mitigate the growing threat of piracy in all its permutations, service providers are leveraging the cloud-hosted multi-DRM, anti-piracy and theft tracking services provided through the ExpressPlay Media Security Suite.

A key purpose of this paper is to explain the considerations that go into an objective search for solutions that will do the best job of accommodating eSports providers' security needs. When the focus is on combating content theft and piracy, the process of choosing the best solutions must take into account several factors, including:

- Robustness and thoroughness of solutions
- Flexibility to tailor their solutions for providers
- Ease of implementation and use
- Level of customer support
- Total costs of ownership

This paper begins by explaining the types of security mechanisms that eSports producers and distributors can implement to combat theft. It then explains how an assessment of these needs leads to the ExpressPlay Media Security Suite as the premium approach to best mitigate these risks.

Basic requirements in eSports content protection

The role of rigorous encryption technology as a first line of defense against theft of downloaded content is well understood in the gaming industry.

In today's digital-first game sales ecosystem, nearly all premium game-hosting platforms prevent unauthorized access to their products through use of encryption in conjunction with platform-specific digital rights management (DRM) systems, which are used to confirm a user's right to play prior to decryption.[1]

Encryption plays an equally vital role in the protection of valuable streamed content although there's far more complexity entailed in the use of DRM technology in streaming applications.

Nonetheless, the time has come for wide scale use of encryption in eSports streaming. This is essential to protecting content from revenue-draining pirate operations whether or not the content is part of a subscription or pay-per-view service. In the case of free services, pirates can easily capture and package unprotected programming to look like it's coming from a legitimate source. When people are fooled into streaming the content from pirate sites, eSports producers and their distributors are deprived of the ad proceeds they would otherwise gain from those users in their viewer counts.

Encryption plays an equally vital role in the protection of valuable streamed content although there's far more complexity entailed in the use of DRM technology in streaming applications.

DRM systems for high-value streaming services

Streaming services traditionally use a variety of low-security protection mechanisms to discourage theft, ranging from simply requiring viewers to use passwords to encrypting the content and passing out decryption keys on an unprotected per-user basis. But with the emergence of high-value streaming services offering broadcast-caliber live and on-demand programming, whether supported by subscription fees, advertising or combinations of both, a far more rigorous mode of DRM-based protection has taken hold.

These state-of-the-art DRM systems separate decryption keys from the content and manage the entire decryption flow in a secure process that can't be accessed by end users. License servers, reacting to requests from authenticated devices by authorized users, securely transmit the keys for decryption on the authenticated device, thereby preventing use of the keys by any other users or the same user on any other device, unless such use is specifically authorized by the provider.

The type of DRM system in use with any given content flow depends on which DRM system is supported by the receiving device. This greatly complicates matters in a highly fragmented device environment.

The multi-DRM mandate

The lion's share of connected devices natively support one of three DRMs associated with the dominant operating systems (OS): Apple FairPlay with iOS, macOS and tvOS; Microsoft PlayReady with every Windows device and some Android devices, and Google Widevine with every Android device and some others.

In order to maximize reach, eSports distributors must also consider other devices that don't support any of the DRMs that have been certified under current licensing policies. As an example, there is a vast ecosystem of devices, primarily in Asia, which natively support the open-standard Marlin DRM.

Distributors also must contend with the fragmentation within generations of device OSs, which impact how they interact with OEMs and DRM suppliers to authenticate the devices for access to premium content. To ensure consumers can access content on whatever device is at hand, distributors must be able to sign into the core security embedded in the device OS or in the OEM's chipsets.

The only manageable approach to delivering protected eSports content across this fragmented device ecosystem involves implementation of a multi-DRM platform, which must be able to ensure consistency in user experiences across all devices with delay-free acquisition of keys from DRM servers run by multiple licensing authorities. Otherwise, distributors would either have to maintain separate security silos to protect each asset stream across all devices or restrict access in order to limit the number of silos.

The content protection solution eSports providers need

It's now possible for even the smallest eSports businesses to cost effectively fulfill the multi-DRM mandate, thanks to the innovative use of cloud technology embodied in the ExpressPlay Media Security Suite.

ExpressPlay DRM, the multi-DRM software-as-a-service (SaaS) component of the Security Suite, has been deployed in over-the-top (OTT) streaming service operations globally and can enable multi-DRM workflows with greater technical agility and at less cost than any other approach.

Market-leading functionality at minimum costs

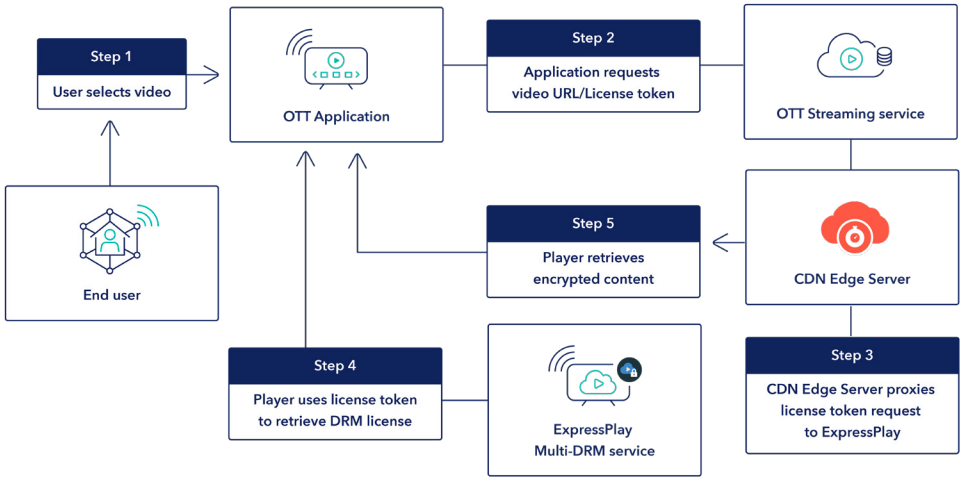
Operating on Amazon Web Services (AWS) facilities worldwide, ExpressPlay DRM makes it possible for eSports distributors to implement robust rights management on a usage-driven cost basis (OPEX) without adding new infrastructure or incurring extraneous setup costs (CAPEX).

The success-oriented fee structure leverages Intertrust's ability to amortize costs across a vast customer base with graduated pricing that reduces per-use rates as total usage increases.

As depicted in Figure 1, ExpressPlay DRM delivers the functionalities essential to covering all the bases of any eSports service strategy. This service offers complete end to end protection, including issuing of DRM licenses, management of content keys and auditing of license acquisition events.

The ExpressPlay DRM service can be tightly integrated through standard APIs with any private or public cloud-based encoding platform to provide the same level of latency-free protection that is attainable with on-premises encryption equipment.

Figure 1
ExpressPlay DRM workflow



Extensive optimization of protection for live-streamed eSports

ExpressPlay DRM has been optimized for live streaming through multiple approaches to mitigating the latencies frequently incurred with other multi-DRM solutions. This starts with the elimination of encryption-related delays through the aforementioned tight integration with third-party encoders.

This goes hand in hand with ExpressPlay DRM's ability to execute the fast, efficient Content Encryption Key (CEK) acquisition process enabled by the MPEG-DASH Industry Forum's Content Protection Information Exchange (CPIX) standard. Addressing HLS as well as DASH, CPIX facilitates streaming of protected content to every type of device with use of a common API structure that eliminates the need to rely on proprietary DRM APIs to handle the information exchanges.

ExpressPlay DRM also makes it possible to avoid session startup delays that can occur with issuance of licenses in the user authorization process. Reliance on persistent rather than non-persistent licensing is a fundamental starting point. Persistent licenses continually enable playback from a given service by the licensed user throughout the life of the license, whereas non-persistent licenses terminate with the completion of each session.

Even so it is necessary to prevent delays during the initial license delivery. ExpressPlay DRM offers such an option through a so-called proxy-based license delivery. Rather than relying on token-based license delivery, which requires two roundtrip communications between the player and the licensing source, the proxy model license delivery model enables players to directly retrieve a DRM license from the ExpressPlay service. Licensing authorization through License Proxy is performed as part of the license acquisition process triggered by the player when it detects that a content key is needed, greatly simplifying support for complex use cases such as key rotation and/or multi-party packaging workflows.

Persistent licenses continually enable playback from a given service by the licensed user throughout the life of the license, whereas non-persistent licenses terminate with the completion of each session.

Essential support for monitoring content theft and combating piracy

While comprehensive multi-DRM protection is essential to minimizing illegal use of eSports content, eSports providers will want to take additional steps to combat the rampant piracy.

First and foremost, eSports providers should know to what extent, if any, their revenue flows are being impacted by piracy. This requires some way to know when and to what degree content theft is occurring by quickly identifying any streams emanating from unlicensed sources.

Should it turn out that persistent monitoring shows that the level of theft is exceeding a provider's pain threshold, the next step would be to implement a means of identifying the pirates in order to facilitate disruption of their output and any legal action that might be taken to shut them down.

This is accomplished through insertion of indiscernible digital coding, known as forensic watermarks, that associate each stream with a specific recipient. In the case of eSports, this must be done by using methods that are conducive to disrupting pirated service in real time and as it occurs to protect and maximize live event revenue.

Here, again, the solution lies with cloud-based technology embodied in the ExpressPlay Media Security Suite. In this case, the platform provides the most effective means available both for monitoring content theft and for employing watermarking to effectively combat eSports piracy. At the same time, it delivers the same SaaS cost efficiencies with these applications that come with use of ExpressPlay DRM.

In the case of eSports, this must be done by using methods that are conducive to disrupting pirated service in real time and as it occurs to protect and maximize live event revenue.

A comprehensive approach to monitoring content theft

When it comes to monitoring content theft, the Media Security Suite utilizes web crawling tools in conjunction with digital fingerprinting technology, a mainstay in automatic content recognition (ACR) applications. In this case fingerprinting is used to identify licensed content that isn't coming from licensed sources.

Digital fingerprinting, as the term is used in media, entails storing a few key video and/or audio descriptors which, together, uniquely define a piece of content licensed to a specific distributor. If automated scrutiny of server-stored content licensee listings shows the content isn't coming from an authorized source, the content is immediately flagged as stolen.

Watermarking optimized for live-streaming environments

The live stream-optimized watermarking solution available through the Express Play Media Security Suite has become the go-to option worldwide as providers of live-streamed content increasingly feel compelled to find an effective way to disrupt illicit user experiences. Recourse to watermarking in live sports streams has expanded rapidly in the wake of results demonstrating that awareness of the risks of disruption has a significant impact on consumers' appetite for pirate services.

The live stream watermarking solution available through the ExpressPlay Media Security Suite makes it possible for license holders to disrupt viewing of stolen content within a few minutes after streaming starts.

The solution accomplishes everything that needs to be done to get these results, including:

- Rigorous resistance to pirates' detection of watermarks and any efforts to circumvent them
- Avoidance of any degradation of watermarks or content through all phases of distribution prior to or after theft
- Execution of watermarking without having to decrypt and re-encrypt protected content
- Support for extraction of the marks directly from the video for immediate identification of pirate sources (eliminating traditional "non-blind" approaches to detection that require comparison with the original unmarked video)

Mitigating eSports app vulnerabilities to malicious disruptions

Shielding eSports apps against reverse engineering, tampering, cloning, and the other lines of attack requires modifications to the apps themselves through a variety of techniques that can be employed during the initial app development process or through adjustments to an existing app.

Shielding eSports apps against reverse engineering, tampering, cloning, and the other lines of attack requires modifications to the apps themselves through a variety of techniques that can be employed during the initial app development process or through adjustments to an existing app.

Code obfuscation

The set of primary defenses that's essential to protecting eSports apps against unwanted reverse engineering falls under the general category of code obfuscation. Such methods range from basic techniques widely employed by developers to more complex modes of obfuscation that are employed much less frequently. In all cases, the goal is to make the code as confusing as possible to reverse engineering tools without altering app functionality in any way. This is predicated on the well-established principle that the more time-consuming and complicated it is to unravel obfuscated code, the less worthwhile it is for hackers to try to reverse engineer it.

Anti-Tampering protections

A second broad category of techniques essential to shielding eSports apps embodies anti-tampering protections, also referred to as runtime application self-protection (RASP).
These in-app mechanisms are designed to complement obfuscation by preventing hackers from installing rootkits and backdoors, disabling security monitoring, subverting authentication, and injecting malicious code that logs keystrokes, steals data, escalates user privileges, or performs other malicious actions.

Protection against attacks on cryptographic operations

Beyond the direct app shielding techniques, comprehensive app security for eSports providers entails implementation of protections preventing misuse of app encryption keys and deterring what is known as side-channel attacks.

Hardening in-app cryptographic keys

The need for cryptographic key protection stems from the fact that developers frequently use encryption to protect critical in-app functions, which can only be activated by clients when decryption is enabled by encryption keys.
The problem is that these keys, as opposed to the keys used with DRM to decrypt the content, are typically hard coded into the app.

As a result, when hackers execute reverse engineering or other app tampering methods they can access and make use of the encryption keys. This renders the encryption pointless unless the keys are protected.

Countering side-channel attacks

Side-channel attack vulnerabilities pertain to the ability of hackers to execute attacks in any OS environment based on observations of the characteristics and behavior of devices as they perform cryptographic operations. For example, hackers have access to sophisticated processes that can read and mimic key algorithmic processes without ever cracking the code. They can do this by monitoring and analyzing patterns related to electromagnetic emissions, thermal energy, power consumption or timing often in conjunction with speculative execution of attacks using the narrowed field of algorithmic possibilities.

In all cases, the goal is to make the code as confusing as possible to reverse engineering tools without altering app functionality in any way.

Conclusion

Vulnerabilities to content theft and attacks of eSports streaming platforms leave no doubt that eSports producers and distributors must find adequate modes of protection on both fronts.

This requires an understanding of the types of mechanisms that have been developed to meet these needs with an eye toward ensuring that the approaches taken are not only the best at accommodating the requirements, but do so with the least impact on staff time and budgets.

Intertrust has developed the solutions eSports providers need to satisfy these criteria. Through the SaaS support offered with the ExpressPlay Media Security Suite, eSports services can benefit from the low-cost, turnkey multi-DRM, theft tracking, and anti-piracy solutions that are already protecting live-streamed sports and other streaming services worldwide.

In all cases, these fully realized solutions relieve eSports providers of the hassles they would otherwise incur with execution of essential protection mechanisms. These solutions are complemented by ongoing professional support provided through Intertrust service teams, which ensure eSports providers will be able to stay ahead of the evolving threat scenarios at minimum costs as upgrades and new advancements are introduced.

Clearly, the new age in eSports brings with it a new level of vulnerability to malicious activities that can drain revenues, disrupt business operations and wreak havoc among eSports viewers and competitors. Fortunately, just as clearly, eSports providers have recourse to the full range of cost-effective ExpressPlay solutions they need to secure the successful outcomes that lie ahead.

1 Engadget, We're All Kinda Fine with DRM Now, February 2020

intertrust®

Building trust for the connected world.

Learn more at: expressplay.com/products
Contact us at: +1 408 616 1600 | onestopshop@expressplay.com

Intertrust Technologies Corporation
400 N McCarthy Blvd, Suite 220, Milpitas, CA 95035