irdeto

Piracy in the streaming world:

Understand what you are facing

Piracy – the biggest rival of the video entertainment industry – has become more rampant!

Piracy today has grown into a profitable business rather than a spontaneous act for individuals to be able to watch their favorite video content for free. No more low-quality cam releases, pirates now deploy cutting-edge technical methods to intervene in the deep-down information processing of the service providers, easily stealing high quality videos and redistributing them on the internet.

No party in this industry is safe from pirates' hands. Due to its astounding growth, the Over-The-Top (OTT) sector is becoming the number one target. Countless well-invested pirating techniques have been created to attack OTT service providers, the most common of which include credentials theft, content key decryption, session token stealing and geo-blocking circumvention.

Before you fight them, let's learn about them. This e-book will provide you with all the insight you need to fully comprehend these popular pirating techniques.

Table of Contents

Piracy in video entertainment: What is going on?

1. HOW BIG IS PIRACY?

i. Why is it important to fight it?

The answer is simple if we look at alarming statistics demonstrating the explosive growth of piracy in the entertainment world. The number of global pirate site visits reached a new record of 215 billion across all media sectors in 2022 – an 18% increase compared with the previous year.

Video entertainment is the most affected industry. Approximately 130 billion visits were recorded for 2022 when examining piracy demand for over 450,000 films and TV series. Access to pirated premium content is easier than ever, thanks to the rise of piracy!

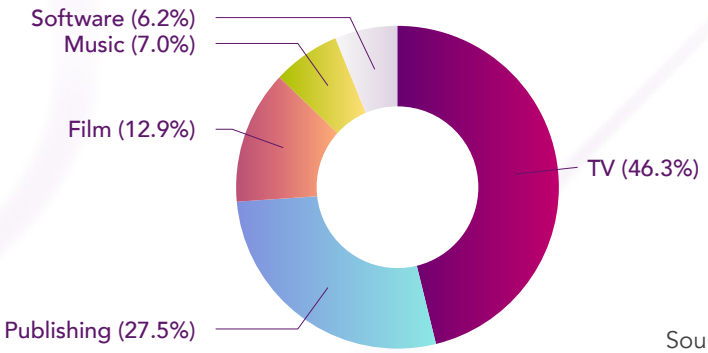
The negative impacts brought by piracy on this industry are immense for both production and distribution. In the US alone, film production suffers yearly losses of between $12.4 and $40 billion, while distribution's revenue losses are from $900 million to $2.1 billion annually. The digital TV sector also has comparable experiences, with annual losses ranging from $14.7 billion to $35.7 billion for production and between $1.3 billion to $3.1 billion for distribution.

The damages are not only limited to revenue but also to the employment within the video entertainment industry. The digital video piracy resulted in between 230,000 and 560,000 job losses in these fields annually.

ii. What content is mostly pirated?

In 2022, TV series and films unfortunately make up the majority of pirated content on the internet with nearly 60%, preceding music (7%), software (6.2%) or other publishing mediums (27.5%). Television shows, series, on-demand movies, anime productions (series and features), live sport events and sports channels are the most frequently pirated genres.

Share of 2022 Global Piracy Traffic

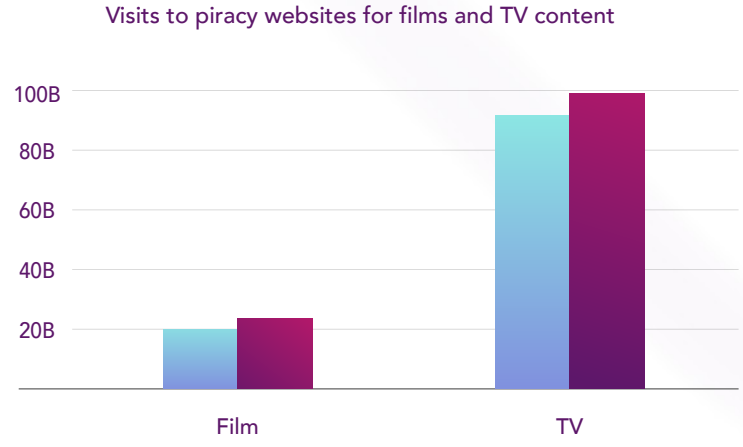


Source: MUSO

In particular, TV piracy accounted for over 46% of global piracy traffic (nearly 100 billion visits) – highest among all categories – while films came in third with about 13% (27.8 billion visits).

Piracy in the film industry surged significantly in 2022, gaining 36% year over year, even though the number of wide-release films still stayed below pre-pandemic levels. Meanwhile, the remarkable spike in demand for anime series and high-profile shows made TV piracy increase by over 9% from 2021.

Film and TV Piracy Growth YoY



Source: MUSO

Meanwhile, the piracy of live sporting events also demonstrated an increased tendency in 2021 and 2022, rising by 30% in just one year. The demand for live sports piracy services tends to spike in April and September, presumably because Europe's top football leagues reach their seasonal viewing peaks during these periods.

2. PIRACY HAS MOVED ONLINE!

i. Online streaming platforms are becoming targets for pirates

In an era dominated by online streaming, OTT services have emerged as the go-to choice for entertainment. By the end of 2023, a staggering 3.8 billion individuals are expected to be using OTT platforms, up from 3.26 billion in 2022.

Attracting many viewers encourages service providers to keep their library of content fresh by constantly adding new TV series and films. This, however, makes them an extremely attractive target for pirates.

In 2022, 95% of TV series and 57% of film content were available on pirated sites. If the current state persists in coming years, the streaming video sector is projected to lose $113 billion of revenue in the US market alone by the end of 2027, according to Parks Associates.

ii. Why are OTT services so easily attacked?

The rampage of pirates in the OTT sector is made possible by a number of causes. The first thing that needs to be mentioned is lower physical barriers, especially when compared with pay-TV. While a Set-Top-Box (STB) is a managed device on a managed network with the support of Conditional Access System (CAS), encryption and secure protocols, streaming services are more vulnerable when using an unmanaged network on unmanaged devices, like smartphones, tablets or computers.

Secondly, despite the benefits of Digital Right Management (DRM) solutions in providing premium content with extra protection, this method also faces challenges from the fragmentation of the OTT market. Streaming services can be accessed via a wide range of devices, platforms, browsers and operating systems. Each of these could have its own set of specifications in terms of DRM and encryption. It is therefore challenging for OTT providers to distribute their material to all users without the risk of being compromised.

Last but not least, widespread internet-based distribution plays a crucial role in the sharp increase in digital video piracy. Pirates can exploit vulnerabilities in streaming protocols or employ screen recording software to capture and store the content for unauthorized distribution. Nowadays, nothing can stream information faster than the internet. With a huge number of internet users around the world, pirates can easily lure viewers to their illicit services.

3. WHAT DAMAGE WILL PIRACY CAUSE FOR OTT PROVIDERS?

OTT providers today experience significant losses due to piracy.

Losing revenue

All aforementioned methods lead to one common consequence for streaming providers: a huge drop in the number of legitimate subscribers.

Attackers and unauthorized users may have unlimited access to the services (thanks to piracy techniques and credentials theft), making it simpler for them to watch and redistribute premium content without any trouble. When users consume valuable content without paying, OTT providers lose out on potential revenue as well as opportunities to convert and attract new subscribers.

Increasing costs

In addition to losing out on legitimate users, the OTT provider is also inadvertently utilizing their backend resources and third parties' services to dispense licenses and provider services to unauthorized users. This leaves them facing skyrocketing Content Delivery Network (CDN) costs (i.e., CDN leeching).

Lowering service quality

Furthermore, a drop in service quality has a negative effect on paying subscribers' user experiences, particularly as a result of credentials theft, where the number of concurrent users surpass the platform's expected capacity. OTT providers may find themselves unable to support this influx, leading to a range of issues such as buffering, blackouts and other frustrating interruptions. The surge in concurrent users strains the resources of the streaming service, including server capacity, bandwidth and other essential components.

Losing access to premium content

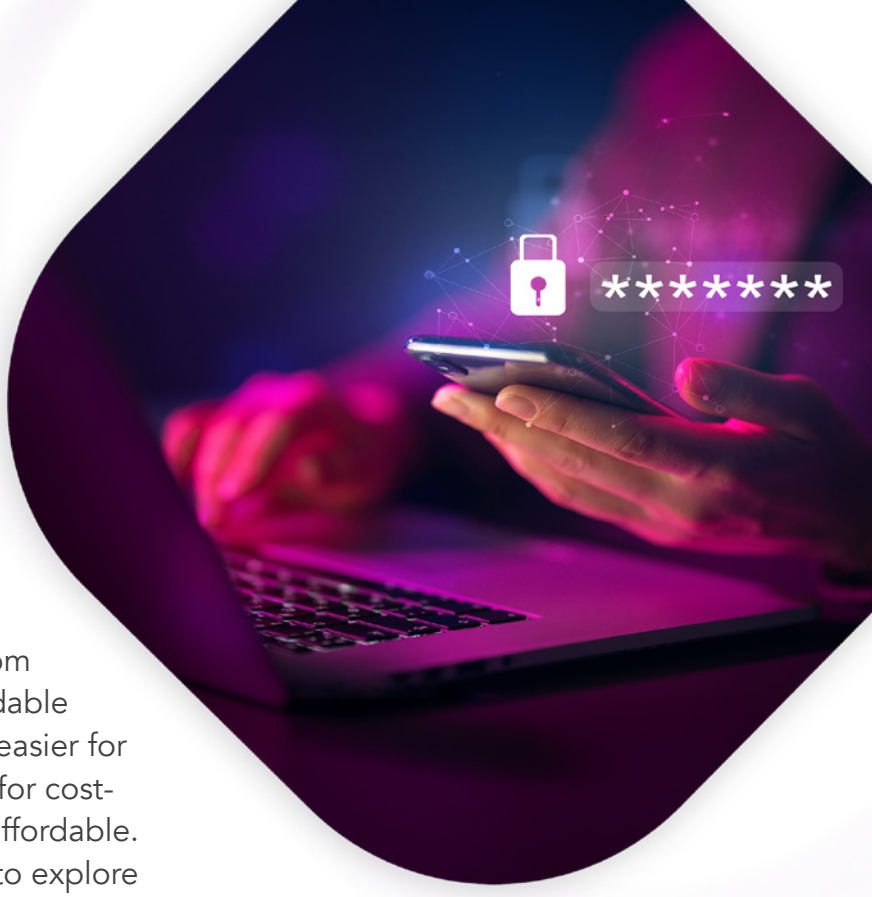
The provider may also be subject to penalties, or even worse, lose access to premium content due to improper compliance with security requirements from both studios and sports rights holders. It may also lead to an increase in subscription churn.

Dealing with such piracy issues is, however, still a complicated task and can end up causing service providers more harm than good if not handled properly. A 'blanket approach,' like revoking compromised devices from accessing video content to combat piracy, would be highly impactful both to their legitimate subscribers and the service provider. Millions of authorized subscribers could see their service cut off, generating customer frustration and flooding call centers with complaints, potentially resulting in churn and tarnishing the service provider's reputation.

Piracy today: Understand what you are facing

It is essential for streaming service providers to understand how pirates nowadays steal content. From simple practices like credentials theft to far more sophisticated techniques, such as content key exploitation, session token hijacking or Virtual Private Network (VPN) usage, pirates know how to undermine the OTT providers' business model and profit from it.

In this section, we will examine their methods in further detail as well as the recommendations to prevent them from happening.



1. CREDENTIALS THEFT

i. What is credentials theft?

Password sharing has become a common practice nowadays for stream services' users. By 2022, 40% of internet users in the US exchanged credentials or utilized shared credentials from others, up from 27% in 2019. This trend is understandable when it offers convenience, makes it easier for people to access content and allows for cost-sharing to make subscriptions more affordable. Password sharing also enables users to explore different libraries without subscribing to multiple services.

Password sharing, however, is not always risk-free and potentially poses a risk of credentials thef. In addition to sharing passwords with the inner circle, like family members or close friends, many people accept sharing accounts with strangers to reduce the cost of entertainment. This gives criminals the chance to obtain users' login credentials and other private data, bringing not only security risks to users but also the threat of piracy to streaming providers.

Moreover, widespread password sharing also presents significant financial challenges for video streaming companies. Recent research found that each shared account can consume premium content 177% more than genuine accounts by being able to serve up to 2.75 households. In other words, shared accounts unfairly increase an operator's infrastructure expenses and limit their capacity to develop fresh content and maintain a competitive edge.

This requires streaming providers to have strategies to address various password-sharing purposes.

ii. Recommendations

Addressing the topic of password sharing, however, can be challenging for OTT providers due to customer frustration and the risk of subscriber churn. Additionally, concerns about increased costs and a perceived loss of freedom further complicate the issue. What should OTT providers do to appease their customers and protect their premium content?

Firstly, OTT providers should introduce more personalized and user-friendly plans. This approach will help them capitalize discouraging password sharing, creating the opportunity for investment in technological advancements to improve streaming capabilities, ensuring faster streaming and steady playback. This is what a streaming giant – Netflix – successfully implemented. The company released earlier this year the "Extra Member" feature, where consumers can enroll additional family members or friends outside of the household for a small extra fee, limiting account and password sharing between users.

Secondly, applying Concurrent Stream Management (CSM) solutions is highly necessary. This technology provides a mechanism to control credential sharing beyond a certain limit as considered legitimate. Providers can ensure that their services are not abused by identifying unauthorized access if users' credentials are compromised and then revoking them. This method strikes a balance between preventing excessive sharing and maintaining a positive user experience, which is crucial for the long-term success of any OTT service.

To achieve these two points, it is equally important for streaming service providers to look for a flexible multi-DRM system that allows them to use CSM to tailor different business plans, such as region-, content-, device-focused or combination of these. This is a feature that not all DRM solutions on the market can offer.

2.CONTENT KEY DECRYPTION

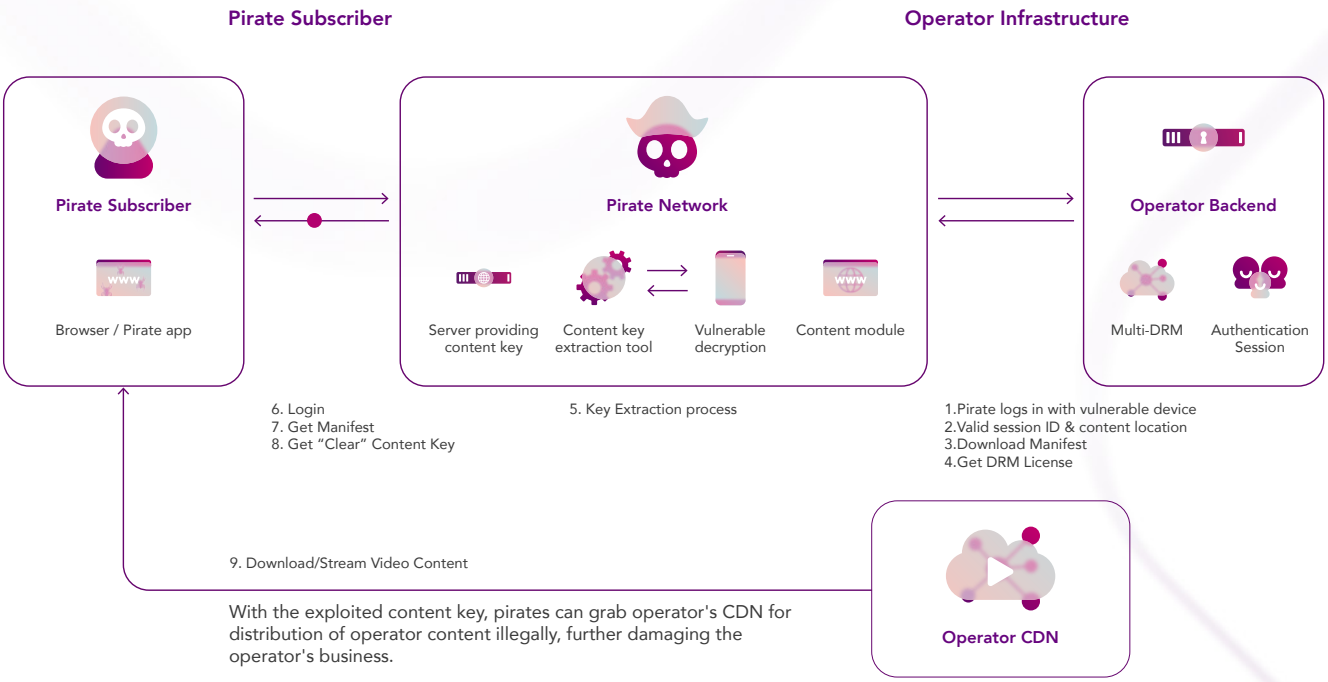
i. How does content key extraction work?

Most streaming service providers rely on DRM solutions to encrypt their premium content in order to stop pirates from freely distributing it. The DRM framework is designed to protect the keys used to encrypt the content from being exposed, even to the user. As a result, the process of client-side server retrieving a license with decryption keys is required to unlock the content and enable the user to watch their premium selection.

The DRM offers different levels of content protection depending on whether it uses hardware or software security. The former provides the highest level of protection since cryptography and media processing operations occur inside a Trusted Execution Environment (TEE). With the latter, the protection is reliant on the software DRM being embedded into the Operating System (OS) without a TEE to run the encryption, making the device prone to hacking and breaches.

For that reason, many devices in use today that lack hardware DRM protection and rely solely on their OS protection are more vulnerable to content key extraction.

How does content key extraction work?



With access to vulnerable devices, pirates can easily bypass the content decryption module and extract the content keys using decryption tools widely available online. The keys are then publicly shared on pirate sites. As a result, any internet user can access premium video content without paying a subscription fee to the service provider.

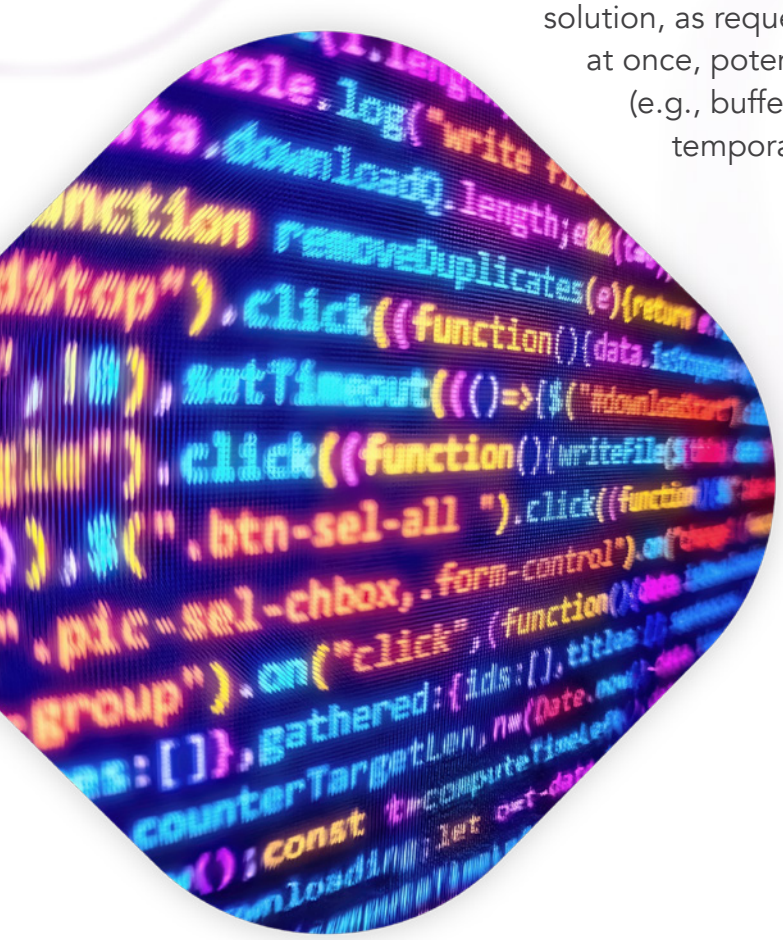
Furthermore, premium content being freely accessible also leads to a huge loss in revenue and increased content delivery network costs for the OTT service.

ii. Recommendations

There are a few recommendations for OTT providers to prevent content key decryption from happening.

- Using hardened software DRM: With this approach, the content decryption bypasses the device's OS software DRM, taking place inside the video application itself instead. When taking this approach, it is best to harden a non-proprietary hardware DRM. It is a cheaper and faster method since the providers do not have to set up a new server and pay to use the proprietary DRM, avoiding costly custom integrations. Its renewable security provides increased agility, deploying quickly and responding efficiently to piracy attacks. It protects against pervasive threats to software security, including reverse engineering, software tampering, copying/cloning and automated attacks, while safely encrypting and decrypting data and communications.

- Utilizing key rotation: Key rotation is a security measure that prevents key factoring and key redistribution by limiting the number of messages encrypted with the same key. In order to prevent pirated sports or other high-profile live events from being watched in their entirety, the content key should be switched over a period of time, such as every 15 to 30 minutes. To make this method feasible, streaming service providers need a scalable DRM solution, as requests for new keys for all users will arrive at once, potentially causing a poor viewing experience (e.g., buffering or stream stopping) as the server is temporarily overloaded.



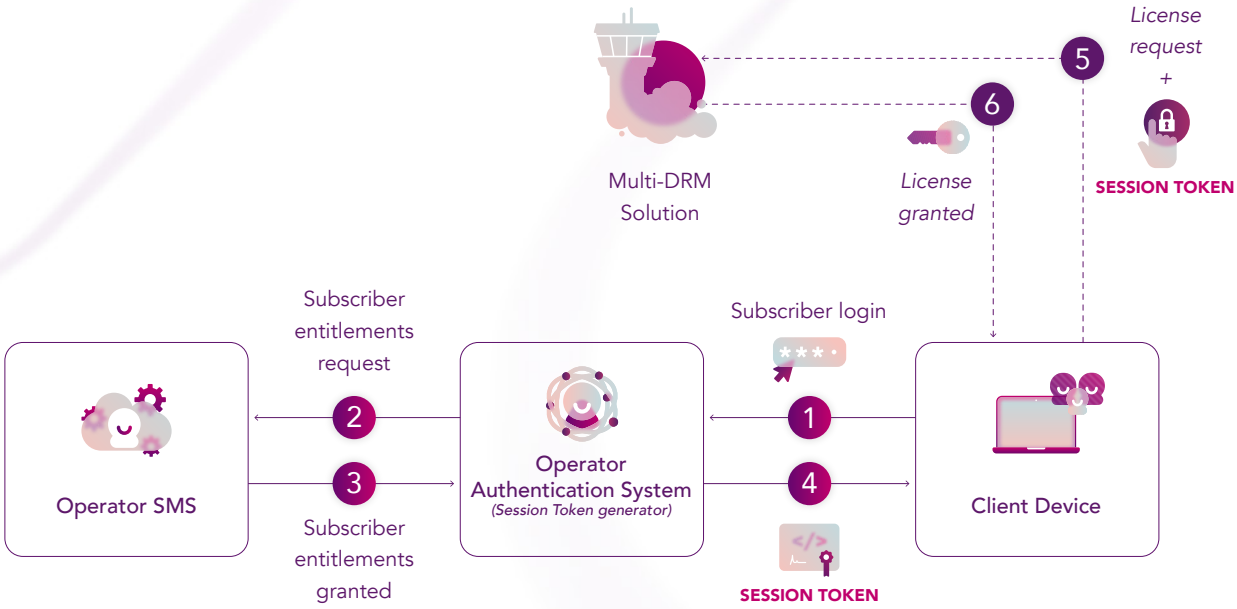
3. SESSION TOKEN THEFT

i. What are session tokens?

If the content key is crucial to the decryption and unlocking of the chosen videos, the session token serves as the foundation for this process.

When a user logs into the OTT service using their credentials, the portal will return authentication proof, typically in the form of a session token – digital certificate that contains the subscriber's unique ID and entitlements. The multi-DRM solution uses session tokens to evaluate the subscriber's rights, granting an access license to a specific piece of content. The following process demonstrates, in a simplified way, how they are generated and utilized.

How session tokens are used



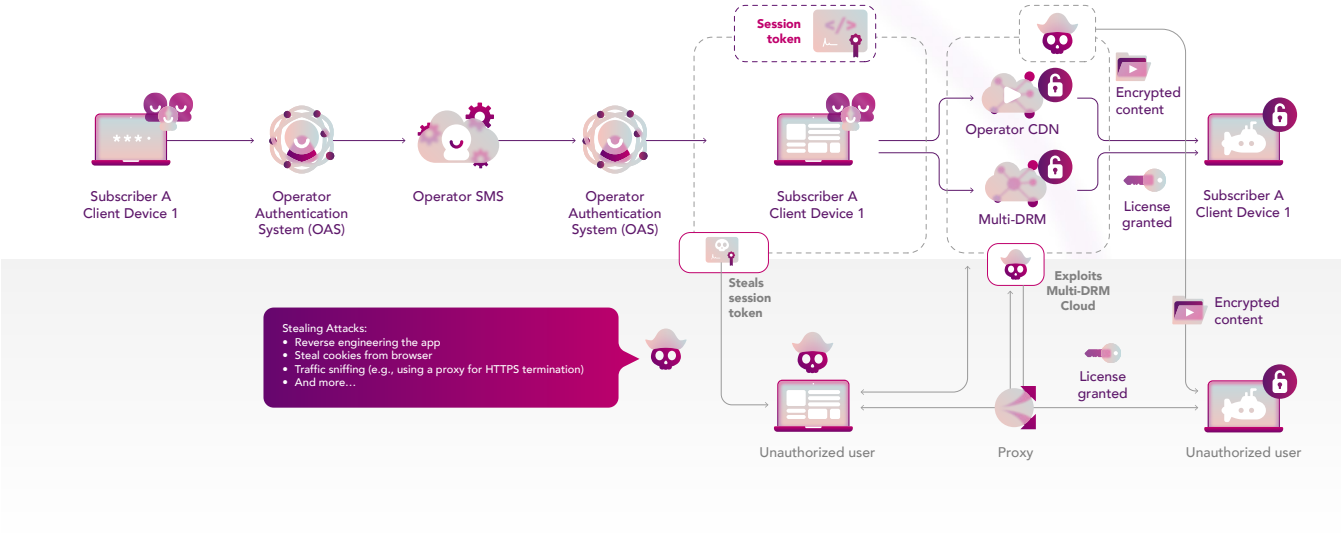
Every time a new request is made, the user's device sends this token to the server, allowing it to validate the token's signature and approve the request.

ii. How do attackers steal session tokens?

Think of a session token as a hotel key card. Anyone with a key card can easily access a specific hotel room and other facilities, making it difficult for the hotel staff to determine whether they are providing services to actual customers. A similar issue can also happen with session tokens and the world of OTT. Linking a token to its legitimate user can be challenging. Once the same session token is cloned to another device, the service provider is unable to detect it.

Furthermore, attempts to steal session tokens become more attractive to pirates when they are valid for a lengthy period of time. This is often the case when providers prefer to use long-duration session tokens in order to simplify their operational infrastructure.

How do pirates steal session tokens?



Stealing session tokens can be done through a variety of means, including application reverse engineering, cross-site scripting attacks or the use of malware that steals cookies from users' devices and traffic sniffing (e.g., using a proxy for HTTPS termination) to name a few.

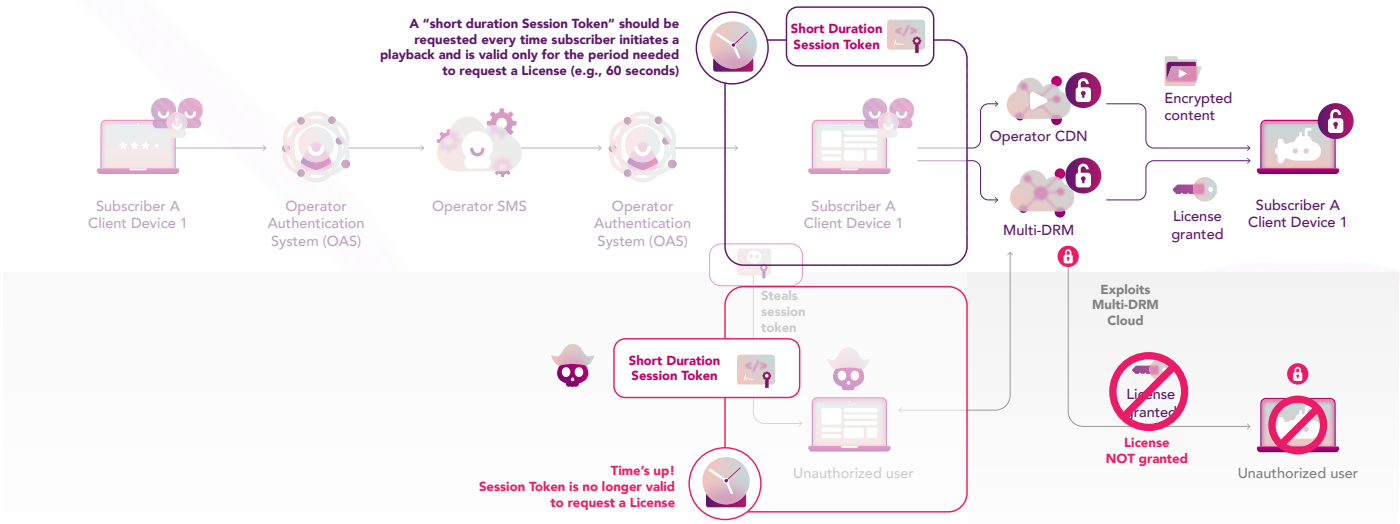
Once individuals with malicious intentions successfully steal a session token, they can access the OTT service and easily commit harmful acts against both end users and service providers.

iii. Recommendations

Session token theft can be avoided by using the following techniques.

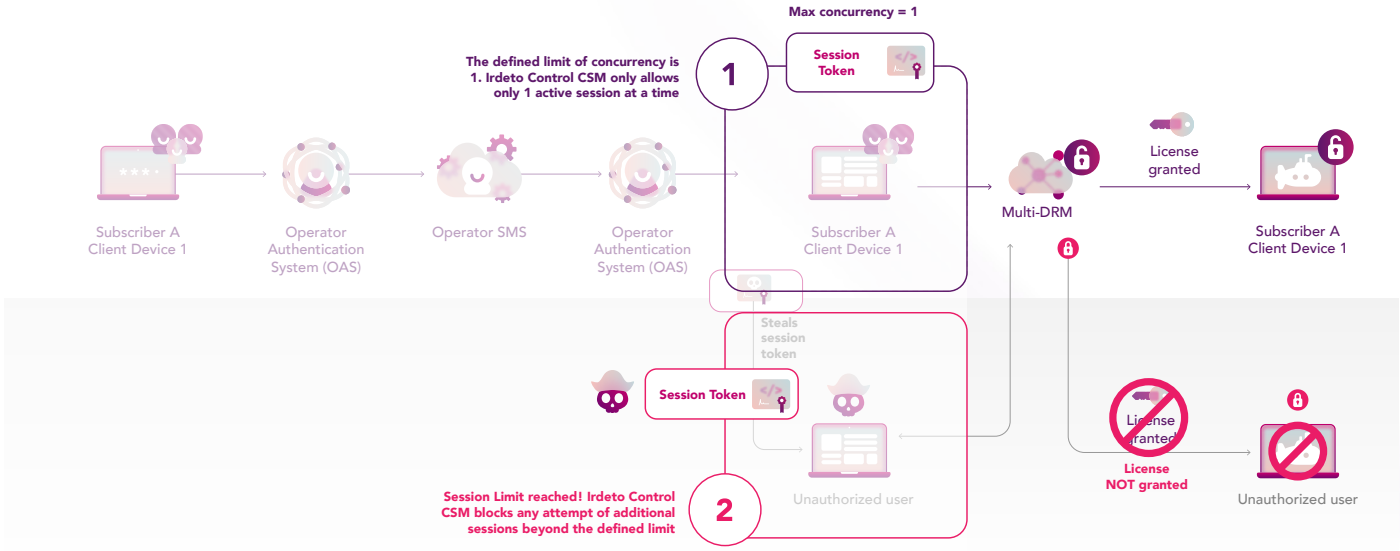
- Short-duration session tokens: The shorter the validity period, the lower the risk. The session tokens should be valid for a limited period, just long enough to exchange an access license between the OTT application and the multi-DRM service. This would discourage unauthorized users from misusing session tokens. The advised validity time for session tokens, however, varies depending on the system and ecosystem specifics.

Short duration session token



- **Frequent rotation of session token signing**: A session token is signed with a 'secret'. Rotating the 'secret' frequently minimizes the probability of reverse engineering token generation/modification.
- **Using DRM-based CSM** to address session sharing piracy: This technology empowers service providers to grow their average revenue per unit by enforcing concurrent stream limits accurately and effectively, preventing revenue loss by discouraging session and credential sharing.

Addressing session sharing piracy with CSM



4. GEO-BLOCKING CIRCUMVENTION

i. VPN providers evolution: Residential VPN

Originally served as a means of providing safe access to the network, nowadays manipulating and making improper use of VPN services has become a popular practice for pirates to circumvent geo-restrictions related to content and usage of the OTT platform. It is not challenging for a streaming provider to identify that somebody is accessing their platform via a VPN and then deny access if required.

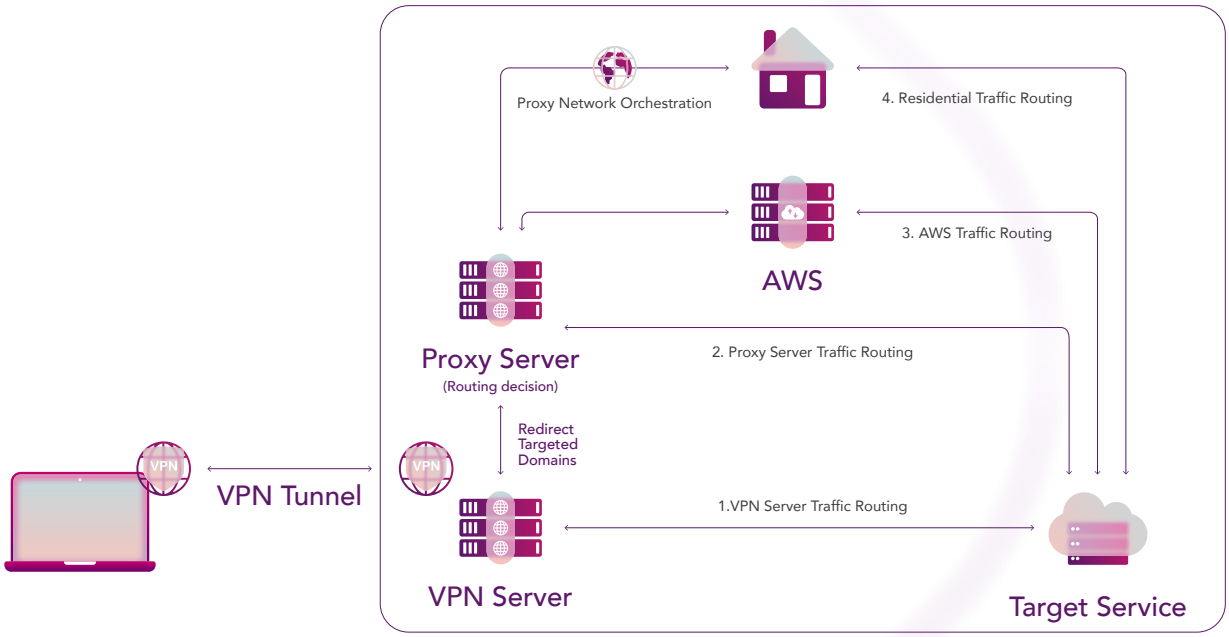
VPN companies that cater to consumers looking to get around geo-restrictions were therefore compelled to evolve and innovate, developing new techniques to make it harder to detect their services. A new kind of VPN provider that touts a residential VPN proxy service emerged as a result.

Even though residential VPN proxy services also utilize hosting data centers, there is an additional hop between streaming services and hosting data centers, which is a residential IP. These VPN providers target regular consumers' residential IP addresses, leading streaming services to only see these IP addresses and are completely unaware of how or who is routing the requests. This is where residential IP hijacking stems from.

ii. IP Hijacking: How it works

Users knowingly/unknowingly have their IPs taken over by these VPN providers when they use free VPN software. The diagram below demonstrates the process of how it occurs.

Residential IP hijacking: How it works



By signing the terms of service without reading them properly, customers provide consent for the usage of their IPs for any purpose by these free VPN service providers. Those providers then leverage the available residential IPs to support the routing of commercial VPN traffic, hence bypassing geo-restriction.

iii. Recommendations

Using concurrent stream management is an effective way to address this issue. If a change in user's IP is detected during heartbeat renewal, this technology can enforce the geo-restrictions as per newly identified IP in the renewal request. Therefore, as soon as a residential VPN/proxy offloads to a cheaper data center IP after circumventing application-level access permissions, its access can be denied by the streaming service provider.

Payment disruption: A powerful defense weapon when your platform is pirated

It is obvious from all the sophisticated techniques above that today's piracy extends beyond small hacks gaining unauthorized access to premium content. It is now even worse, operating as a form of organized crime!

1.THE EVOLUTION OF PIRATE SERVICES

Piracy services are increasingly successful in presenting themselves as legitimate businesses and winning the trust of audiences. In addition to offering the most recent and high-quality content, they also utilize multiple well-known payment provider services, such as bank transfers, credit card operators, digital payment processors or cryptocurrency agents.

Recent statistics discovered that the majority of pirate internet protocol television supplier sites openly promoted their payment options with reputable and legitimate payment institutions. In particular, PayPal accounted for 17.3% of all payment methods, while Mastercard followed in second place with 14.7% and Visa closed behind with 14.1%, according to the Audiovisual Anti-Piracy Alliance's study in 2021.

The issue with this is that the appearance of such well-known brands not only makes it easier to handle payments but also increases consumer confidence in illicit services. This helps them build a veneer of authenticity and convince many unwary consumers to subscribe to their services.

It is not an exaggeration to say that by offering a comparable user experience that appears legitimate at a lower cost, those illegal options are making an attractive offer that not many customers can refuse.

2. WHAT APPROACH SHOULD OTT PROVIDERS TAKE?

A more tech-savvy and sophisticated strategy is required to combat pirates and stop them from distributing premium content illegally. Third-party vendors who possibly inadvertently facilitate the pirate ecosystem, such as banking and financial institutions, should be included to create a comprehensive anti-piracy approach.

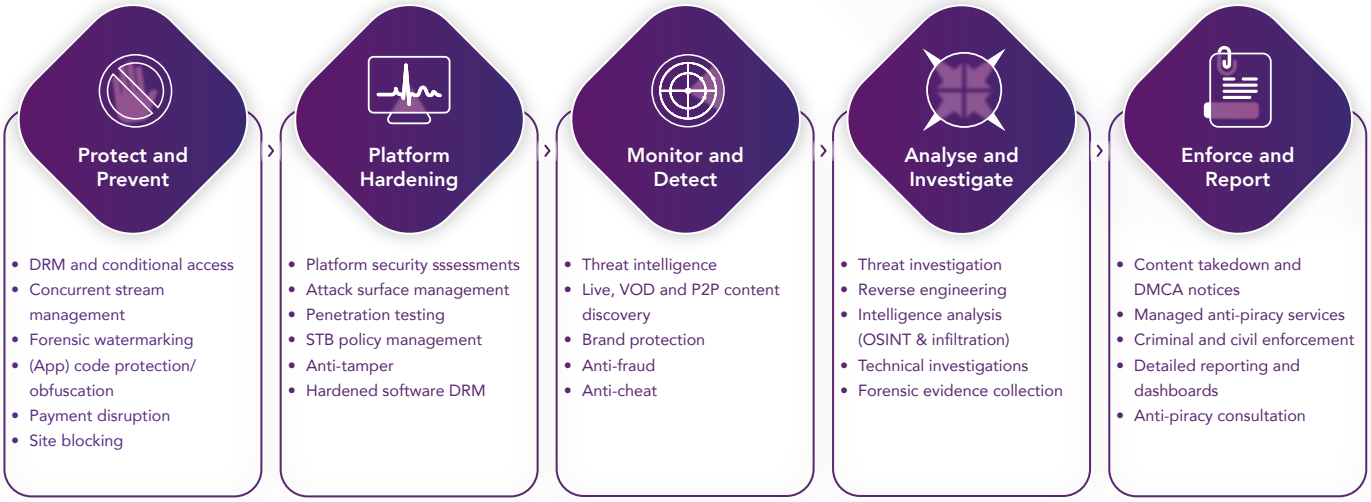
Subscriptions and advertising are how pirates generate money and here is where the industry must focus its efforts. It is therefore critical to disrupt and neutralize their business models as much as possible, leaving them to rely on fringe payment platforms or preferably no payment platforms whatsoever.

By cutting pirates off from using popular and legitimate payment supply-chain platforms, it is increasingly difficult for them to convince or lure potential customers to subscribe to their services, limiting their ability to reach a larger consumer base.

You have anti-piracy needs – we have a solution!

Understanding what you are facing is just the first step in the fight against pirates. To win this battle and ensure a profitable return on investment for your OTT service, it is also necessary to thoroughly analyze your areas of vulnerability and build a comprehensive security plan based on your assessment. By doing so, combined with preparing an end-to-end anti-piracy approach throughout the stages, you can protect your digital assets.

5-step program for Anti-Piracy and Cybersecurity management



The establishment of necessary advanced technologies as well as a strong and massive team of cybersecurity experts to handle each of these stages will, however, cost providers a lot of money, time and effort. As a result, it is always good practice to have a reliable security partner under your arms.

Don’t fight alone

Contact us to put an end-to-end anti-piracy plan together!

irdeto

Protect. Renew. Empower.

Irdeto is the world leader in digital platform cybersecurity, empowering businesses to innovate for a secure, connected future. Building on over 50 years of expertise in security, Irdeto’s services and solutions protect revenue, enable growth and fight cybercrime in video entertainment, video games, and connected industries including transport, health and infrastructure. With teams around the world, Irdeto’s greatest asset is its people and diversity is celebrated through an inclusive workplace, where everyone has an equal opportunity to drive innovation and support Irdeto’s success. Irdeto is the preferred security partner to empower a secure world where people can connect with confidence.