Friend MTS

Content Protection & Anti-Piracy

Glossary

There are many words and phrases that are used to describe the tactics, applications and processes within the content protection and anti-piracy ecosystem.

To make it easier to navigate these and ensure clarity and transparency, we have created a content protection and anti-piracy glossary of terminology for you to refer to, whenever you need it.

A/B variant (watermarking)

A technology that involves preparation of two differently watermarked media segments ('A' and 'B' segments) at the server-side that are then interleaved in a specific sequence of 'A' and 'B' segments at the server-side or at the edge to generate a watermark pattern unique for each subscriber.

Anti-piracy

The action of protecting premium video content from being purloined by pirates (q.v.) in order to avoid financial, brand and reputational damages. Often refers to *monitoring* (q.v.) and *watermarking* (q.v.) aimed at curbing illegal redistribution of content through detection and takedown of pirated content.

App/application hardening

Technology that secures applications (apps) against attempts to circumvent security and to reverse engineer or access content directly, often for the purpose of illegal redistribution. Hardening security techniques include *code obfuscation* (q.v.), white box cryptography, trusted execution environments, tamper prevention and tamper detection.

Bitstream modification (watermarking)

A technology that creates a watermark by modifying a specific area or areas of the video (invisibly to the user). The watermark is applied either at the CDN edge or on the *client side* (q.v.). In either case, server-side pre-processing of the content is required.

Casual piracy

The action of *pirates* (q.v.) illegally obtaining and/or redistributing video without the intent of significant financial gain but rather to save money on subscriptions, viewing content that is not available within their territory, save time on finding the content, share the watching experience with friends that don't have a subscription, etc. cf. *professional piracy*.

Client-side (watermarking)

A technology that generates and applies a watermark (an imperceptible graphic overlay, agnostic to the video) at the point that the content is delivered to the end device, e.g. a set-top-box or OTT player. cf. *server-side*.

Client-composited (watermarking)

A method of blending a graphical overlay with the video – a watermark (an imperceptible graphic overlay, agnostic to the video) in the cloud and applies it at the point of delivery of content, to the end user's application or device (the client). Watermarks can be delivered securely via a cloud-based service usually along with other security technology, such as *DRM* (q.v.), *code obfuscation* (q.v.) or *app hardening* (q.v.); alternatively, the watermarks can be generated by the end-users' device.

Conditional Access System (CAS)

Conditional access systems are used by content providers, such as pay-TV operators, to ensure only those subscriber devices which meet certain conditions can access the protected content. Conditional access systems scramble digital transport streams (the pay-TV content) and separately send authorizations to entitle subscribers to allow the content to be descrambled.

CDN (Content Delivery Network)

A CDN is a network of servers used to deliver content from an 'origin' server to viewers around the world. CDNs are used to ensure high availability of high quality content.

Code obfuscation

Code obfuscation is a security technique that protects applications or web browsers, by altering executable code to make it extremely difficult for hackers or *pirates* (q.v.) to access and/or understand. Code obfuscation is used to protect environments to which content is delivered, such as a media player, application or web browser.

Content protection

The action of protecting premium video content from being purloined by pirates (q.v.) in order to avoid financial, brand and reputational damages. Often refers to *glass-to-glass* (q.v.) protection.

Digital Rights Management (DRM)

Digital Rights Management is a set of access control technologies for restricting unauthorised access to the use of digital content, enabling only legal, authorised content consumption.

Dynamic Delivery Server Blocking

The near-real time action of blocking access to pirate websites carrying illegal content by internet service providers (ISPs), following legal requirements set out in a specific court order issued by a regional court. This anti-piracy measure involves blocking network requests to pirate services by their IP addresses, hence it is also referred to as "IP blocking".

Enforcement

A service often provided in tandem with a *monitoring* (q.v.) service. Enforcement is the process of acting when an illegal source of video content has been located and identified by a monitoring service. Enforcement measures can range from the issuing of takedown notices or DMCA notices to legal action or *dynamic delivery server blocking* (q.v.).

(Watermark) extraction

The process of extracting a watermark payload embedded in content to analyse the information that it contains. When suspected infringing content is located via a *monitoring* (q.v.) service and verified using *fingerprinting* (q.v.), a watermark payload is extracted to reveal the source of the infringing content. Appropriate *enforcement* (q.v.) measures can then be taken.

Fingerprinting

Video fingerprinting is a non-intrusive technique for identifying content based on, for example, the movement observed between video frames. Fingerprinting technology generates a mathematical signature, known as a "fingerprint", that can automatically identify this video among others. Comparing fingerprints between a legitimately distributed video ('reference') and a detected suspect video ('candidate') allows confirmation that the suspect video is from an illegal source. Thus, fingerprinting is used by *monitoring* (q.v.) services to identify illegal instances of content on the internet.

g

Geoblocking

Content protection technology that restricts a user's access to internet-delivered content based on their geographic location, as determined typically by their IP address.

Glass-to-glass

The entire creation/capture and distribution chain for video content, from the camera (glass) to the screen (also glass). Often used in content security to denote full protection of the content from pre-release to the point of its delivery to the viewer. cf. *glass-to-glass and beyond.*

Monitoring (also global content monitoring)

In content security, the process of automated and/or manual monitoring of various digital locations (websites, IPTV services, social media etc.) to locate and identify illegally obtained and distributed content. Monitoring services are often engaged by broadcasters and rights owners who wish to locate and take action against infringing distribution of content that they own. These anti-piracy services are also known as “piracy detection”.

Monitoring platform (also Global Monitoring Platform)

An automated system/platform that monitors for the appearance of pirated content online across various content distribution channels (social media, mobile apps, streaming sites, *pirate IPTV services* (q.v.), illicit streaming devices, add-ons and plugins, etc.). Such a video search and capture system/platform utilises *fingerprinting* (q.v.) to automatically identify illicit video through fingerprint match. Content monitoring platform gathers piracy intelligence, enables IP enforcement including takedown requests as well as forensic evidence gathering for litigation purposes and *dynamic delivery server blocking* (q.v.) in cooperation with internet service providers (ISPs). These platforms are also used to automatically search for the content with embedded watermark payload and capture video for the subsequent *extraction* (q.v.) of watermarks to identify subscription accounts used by pirates to source content.

OTT (Over-The-Top)

Also known as streaming, is a content delivery method where content is delivered over public internet as opposed to broadcast, satellite, cable or IPTV delivery. OTT also refers to any streaming platform that delivers content over the public internet (as opposed to managed networks). Examples include Netflix, Hulu, or Disney+.

Pirate

1. A person who illegally obtains and/or redistributes video, with the purpose of either *casual piracy* (q.v.) or *professional piracy* (q.v.). 2. A disreputable sort who traditionally sailed the seven seas attacking and plundering legitimate trading, merchant or naval vessels. Often has close relationships with parrots, and says "Arrr!" a lot.

Pirate attacks

Attempts made by *pirates* (q.v.) to circumvent content protection measures in order to gain access to premium content with the purpose of either *casual piracy* (q.v.) or *professional piracy* (q.v.). Pirate attacks can range in their complexity from very basic ones like cropping a broadcaster logo out of the video to more sophisticated ones like collusion attacks launched by professional pirates.

Pirate IPTV (service)

An illegal subscription service with an extensive catalogue of premium content aggregating all popular content within one service and offered by pirates for a relatively low fee. Such services often use OTT as a content delivery method rather than IPTV delivery (the name can be misleading). Pirate IPTV services often deliver good quality content, their professional-looking user interface can be hard to distinguish from legitimate offerings and often legitimate payment systems are used. However, such services are not reliable as are a target of content protection and anti-piracy companies and can also present other risks, including cybersecurity ones.

Professional (commercial, for-profit) piracy

The action of *pirates* (q.v.) illegally obtaining and redistributing video with the intent of significant financial gain, for example, through *pirate IPTV services* (q.v.). Such pirates possess advanced technical skills, years of experience and deep knowledge of the content protection landscape that enables them to launch highly sophisticated *pirate attacks* (q.v.) aimed at circumventing content protection measures. Such pirates don't usually work alone but are a part of organised piracy networks that can aid a wide range of other illegal activities. cf. *casual piracy*.

Security audit

A comprehensive review of one's current content and distribution security strategy that reveals where security is strong or vulnerable in order to highlight where improvements are needed to keep a business' data protected.

Server-side (watermarking)

In content security terms, server-side watermarking is the generation and embedding of any type of watermark at the server or CDN edge. cf. client-side.

Visible Watermarking

Watermarking that involves placing a visible/perceptible image over the content. This is often in the form of a broadcaster's or rights holder's logo and/or a distribution platform logo or an individual viewer ID flashed on the screen at certain intervals. This type of watermarking is often used to identify content distributed by a specific distribution platform or partner, or which has been leaked using a specific subscription account. Visible watermarking is a relatively inexpensive content protection method that can be very effective, for example, as a deterrent for *casual piracy* (q.v.). It is, however, not too effective against even simple circumvention techniques (like cropping) used in *professional piracy* (q.v.). cf. *watermarking*.

VPN (Virtual Private Network)

A VPN is a service used to encrypt online data to protect an internet connection and privacy while on the internet. VPNs can be used to make it more difficult to track a user's online activity and steal data. VPNs are also used by video consumers looking to circumvent some security measures, such as *geoblocking* (q.v.).

Watermarking (also Forensic Watermarking, Video Watermarking)

Content protection technology in which a partially visible or imperceptible watermark is embedded into content as it is distributed; the watermark contains unique information identifying the source of the content. The watermark payload can subsequently be extracted from instances of the content that are being illegally redistributed to identify the source. Watermarking comes in different forms which can be deployed at different points of the distribution chain; these include: *client-side* (q.v.), *server-side* (q.v.), *client-composited* (q.v.), *A/B variant* (q.v.), *bitstream modification* (q.v.) and *visible watermarking* (q.v.).

If you found our content protection and anti-piracy glossary useful, read Content Security 101 for everything you need to know