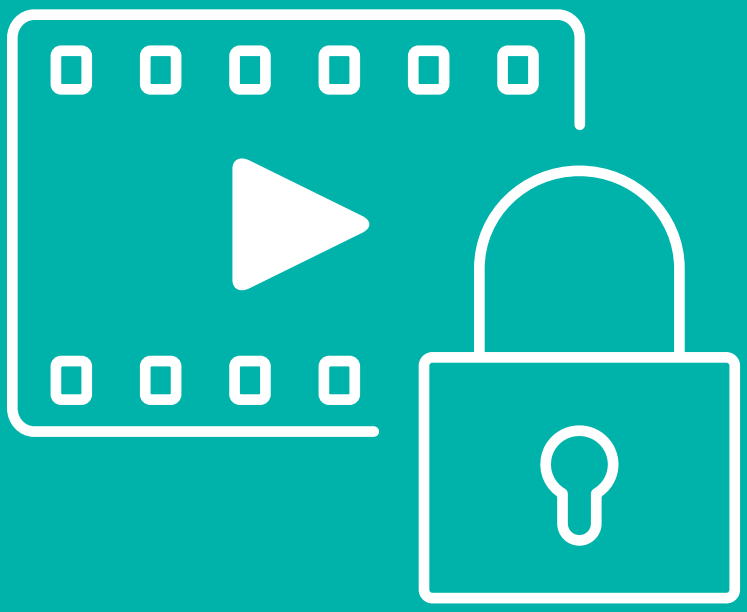
intertrust®

White Paper

Media Solutions

What is DRM?

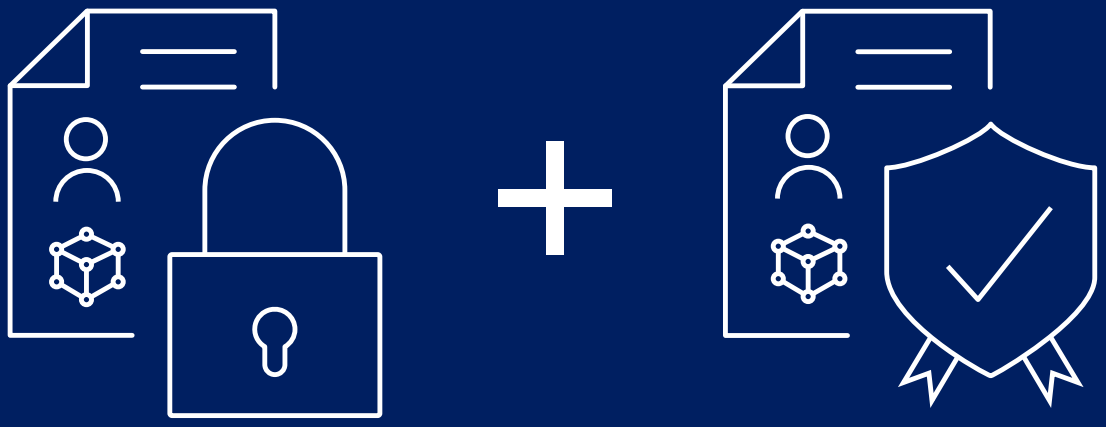


Contents

DRM

Data Protection

Data Governance



Encryption

The process of converting information or data into code, especially to prevent unauthorized access

What is DRM?

As more and more information is being distributed digitally, digital rights management (DRM) technologies are being designed to protect this digital information, which potentially can be copied and redistributed—whether it's done flagrantly or surreptitiously.

DRM consists of two main logical components:

- Data protection
- Data governance

Encryption technologies are generally used to provide data protection, while trust management and policy management technologies are used to protect information from distribution and use by unauthorized entities.

Digital data protection through modern encryption has a long heritage and has been used for many decades, naturally extending from centuries of encryption applications, dating back to ancient cryptography. However, data governance technologies are much more recent, having been deployed only over the past 25 to 30 years. To best illustrate the requirements for DRM and the application and effectiveness of some of the solutions, we will explain these technologies in terms of the challenges they are designed to address.

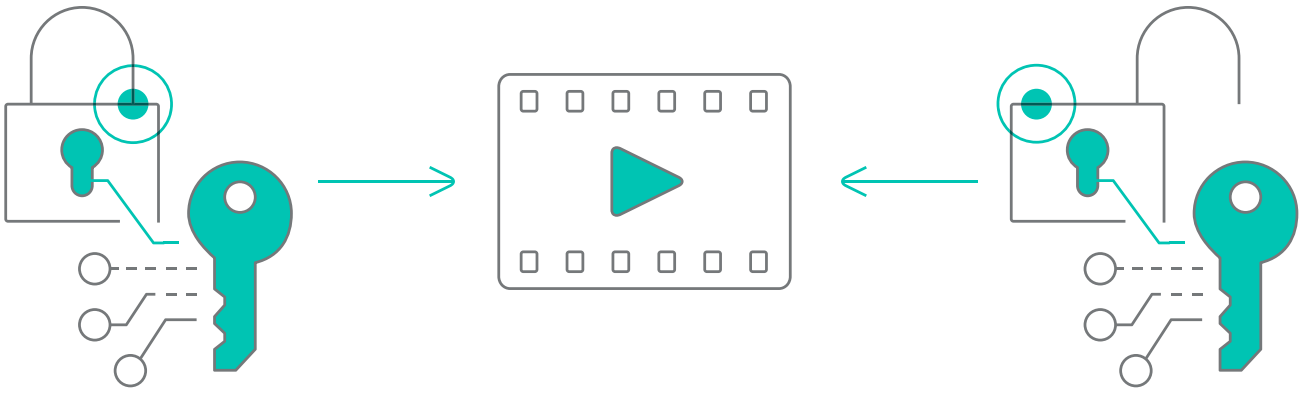
The basics

Once digital information is created, we can keep it in a file, and encryption technologies can be used to effectively protect that file. This is a fairly straight-forward operation. Depending on the nature of the information in the file and the overall goal for protecting it, there are many encryption algorithms that can be used. Sometimes we may care that absolutely no information is discernible from the protected file. In other cases, we only care that the information is commercially unusable, or that the digital asset that the information comprises will not be devalued if used by an unauthorized person. In general, any and all of these goals can be accomplished with readily available encryption technologies and the costs of applying this technology are quite low.

But once the file is encrypted, making the information available in a useful form to authorized parties is a more complex challenge. Today, one can effectively protect a large digital file, such as a music or video file, by encrypting it with a standard cryptographic algorithm using a symmetric key K that is 16 bytes long, much shorter than the file itself. When the key is symmetric, the same key is used to both encrypt and decrypt the file. Therefore, it is critical to protect the key. When we want someone else to legitimately use the file we need to arrange for that party to get access to the key K, while assuring that no illegitimate user can access it.

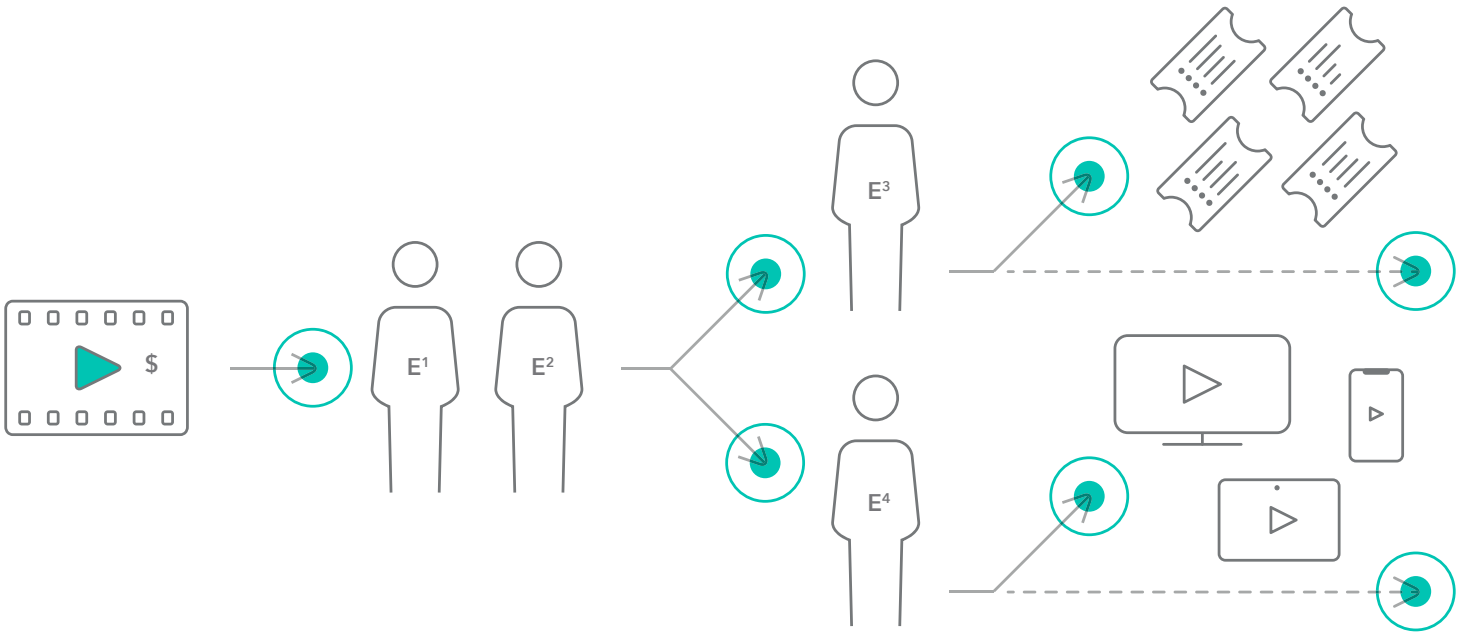
Technologies used to accomplish this are generally referred as key management. Encryption is used in key management since we can protect the key K by encrypting it with a "key encryption key" or KEK. But then it becomes necessary to protect the KEK. To avoid a never-ending, iterative process of keys protecting keys, a technology made available in the 1970s called public key infrastructure (PKI) is used. PKI uses a set of cryptographic keys known as a private and public key pair. These key pairs encrypt information to ensure data is protected during transmission.

When an electronic connection is made, a protected private key is created that is specific to the user making the



Encrypt K

K Decrypt



connection and kept secret. At the same time, a public key is generated and is made available to anyone. During communications, the public (or PUB) key encrypts and decrypts data and the server uses the private key (PRI) to confirm the connection and protect the user's information.

This process can work well, but now there are new issues. We still need to protect K at the source and wherever it is used, including both intermediate locations and the final destination. In addition, we need to make sure that when a party's public key is used, it is their public key and not someone else's. As the universe of potential users grows, this process becomes a bigger challenge.

However, there are still even greater challenges. When a legitimate entity E receives an encrypted file and is able to decrypt it using the process described above, we often want to make sure that E uses the file only for certain purposes and only under certain conditions, ensuring E cannot make the decrypted file available to others without authorization. This presents a much more complex challenge and is the basis for DRM.

DRM involves the application of:

- **Key Management**
  Making cryptographic keys available only to legitimate users
- **Policy and Key Usage Management**
  Ensuring that the key and decrypted information will only be used according to policy under specified conditions
- **Trust Management**
  Ensuring that the entities that handle keys, content, and policy are who they claim to be and will reliably handle the information and execute policy

The challenges above need to be understood when considering the following generic use case:

- We have a high-value asset in a digital file, for example a feature length film that cost more than $100 million to produce, and when properly distributed, has a potential value far greater.
- We need to distribute the file through many different parties. Distribution to each party also involves intermediate entities and distribution points before the file reaches the end users.
- We want to ultimately make the file available at different prices at different times under both sale and rental agreements to many millions of people in theaters or on home and mobile devices sourced from many different manufacturers.

The challenge, which is daunting, is to ensure that the content is not exposed to unauthorized copying and repurposing anywhere along any of the distribution chains during its useful commercial life. There are so many different places where the file might be exposed and placed "in the clear" (unencrypted), and certainly it is the case that this has not been well executed in the past.

In the 1990s, DRM was first used to protect digital music distributed via the Internet. At that time, digital music files were also routinely distributed commercially on CDs, which were without protections. Protecting just one means of distribution—online in this case—ultimately did not make sense when the product was available openly on another.

Furthermore, many different music file formats were prevalent and these varied formats interfered with the consumer experience. Previously, when users bought music content, they could play it on all of their devices. DRM wasn't the only cause of compatibility issues, but it was just one more thing to get in the way. That said, DRM capabilities and conditions have improved consistently and significantly since its introduction, and continue to do so. As we will discuss next, today's state-of-the-art technology protects and governs the distribution of video much more tightly and elegantly, ensuring that DRM does not get in the way of consumers' legitimate enjoyment of content.

Secure systems

A content distribution system has many parts, including components for:

- Content formatting
- Packaging
- Wholesale distribution
- Network staging
- Retail distribution
- Playback hardware
- Playback software

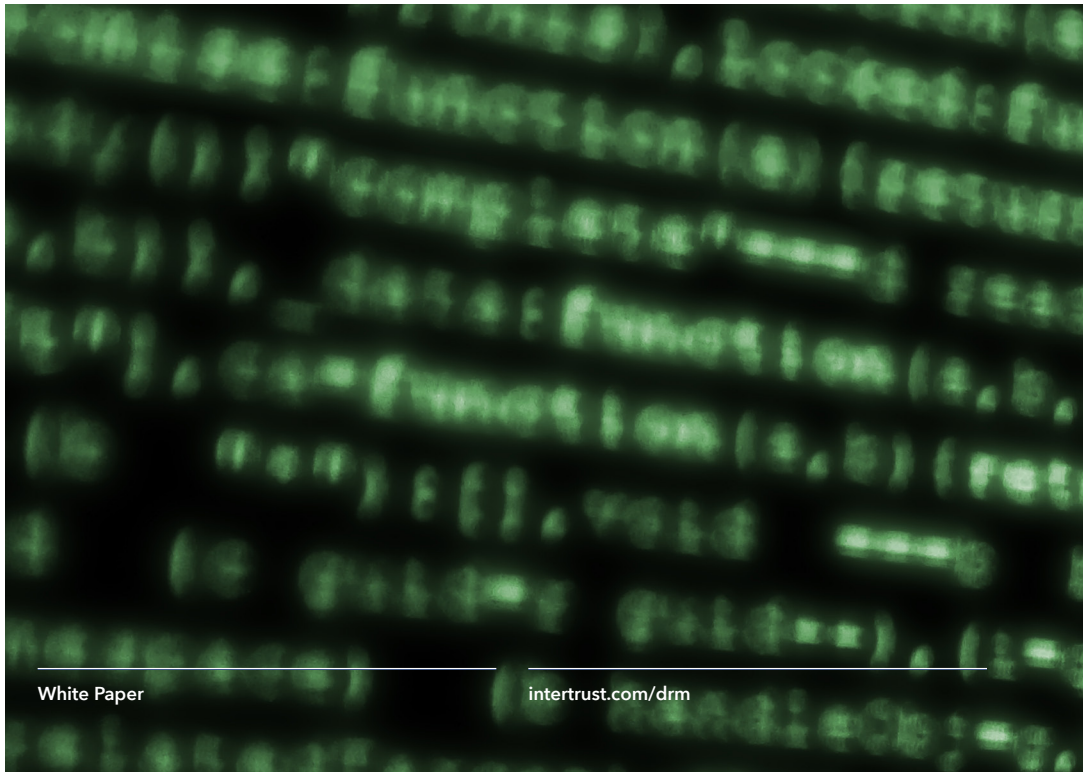
There are risks associated with each of these components, and a secure systems approach to content protection and rights management analyzes and addresses all of those risks.

The more one has control over each aspect of the system, the greater the likelihood of success at fielding an effectively secure system. While it is possible to perform a single operation, such as encrypting a file in a practically perfect manner, given the inherent complexity of the different components and many avenues of attack, addressing all of the risks in a complete content distribution system is not practically possible.

In order to deal with this complexity and help ensure the strongest defense possible, security professionals employ several concepts:

- **Leverage** is computed as a ratio: the cost and risk an attacker incurs divided by the gains from perpetrating a successful attack. In designing a secure system, a high-leverage security solution can make the numerator large, the denominator small, or ideally both.
- **Attack surface (a.k.a. threat surface)** is the set of points accessible to an attacker. Secure systems designers endeavor to make the attack surface as small as possible.
- **Defense in depth** employs multiple methods to address the same risk in order to further reduce it.

We'll discuss these concepts subsequently as we describe approaches to the overall challenge.



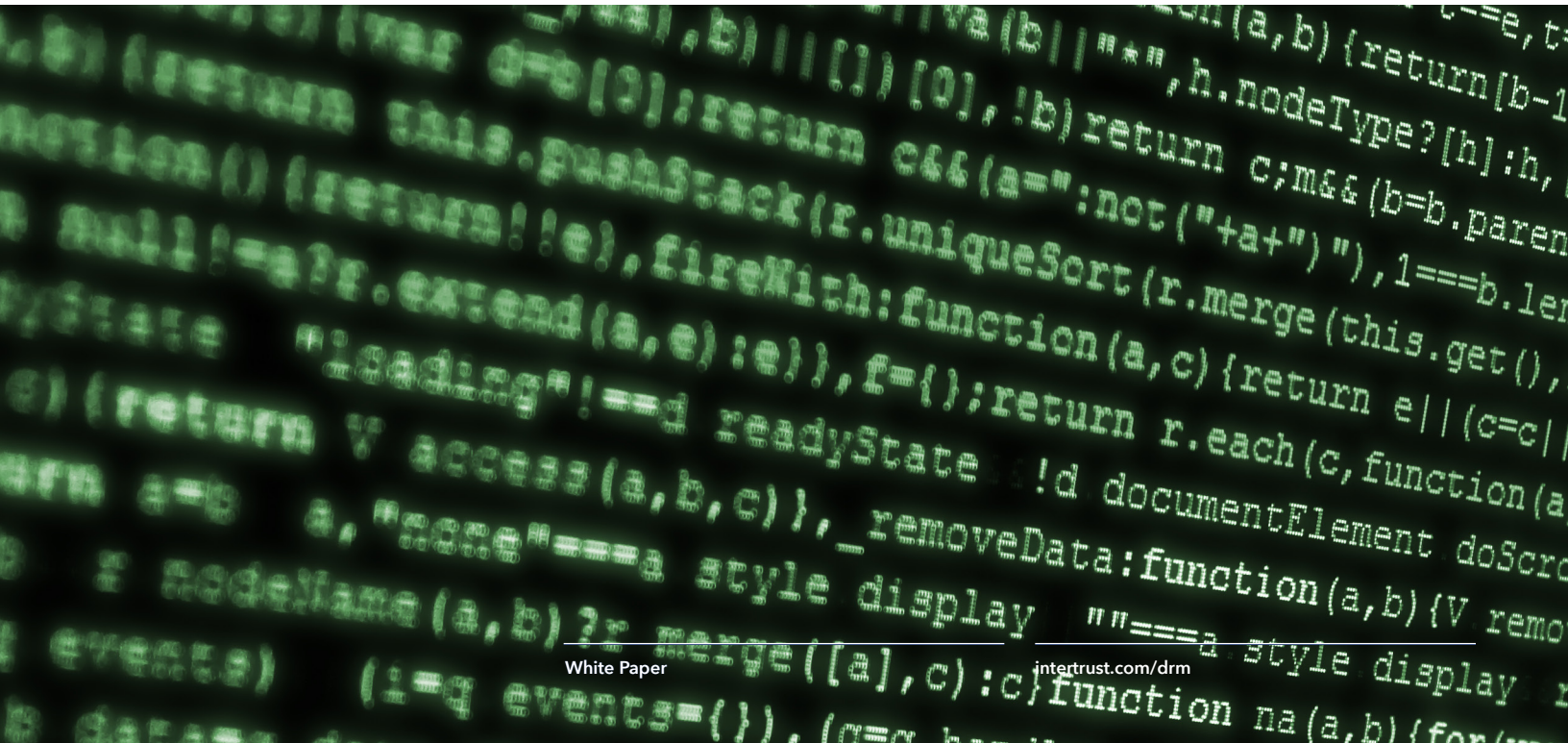
Robustness

DRM implementations need to ensure compliance with prescribed design specifications, ensuring that the protection and decision mechanisms cannot be subverted in specific environments. So "robustness" is a characteristic of a particular DRM implementation, rather than a design, and robustness rules are written to ensure resistance to two types of attacks:

- Reverse engineering of code can reveal an understanding of how the DRM rules and decision mechanisms work, and how they might be subverted. A DRM rule might restrict the use of the content decryption key to a specific time period. The rule is protected using proper authentication technology, and somewhere in the code is a decision that says "conditions are not met, so no-go." Reverse engineering might allow an attacker to determine how and where to interfere with this decision process and thereby undermine it.
- Side-channel attacks occur when a key is obtained not from a break of the encryption but rather through the acquisition of derivative information from "side channels," such as power signals or instruction caches. These "clues" can give attackers ways to infer the key based on the way the encryption is applied.

Software hardening technologies provide two types of defense:

- Obfuscation of the code in such a way that it renders the code extremely difficult to understand.
- Runtime code authentication that detects when the code is attacked, even while executing. This is particularly useful against side-channel attacks.



Deploying DRM

We have shown that DRM includes, among other elements:

- Means for protecting content
- Means for determining trusted components and entities that handle or interact with content
- Rules and policies for using content in unencrypted form
- Robustness rules for ensuring the integrity of DRM decisions and secure use of keys

Next we look at the two overall approaches to DRM deployment.

Distribution silos

Technology providers first emerged as major purveyors of DRM, but only for the sake of their own platforms. Almost immediately, proprietary DRM systems became a means for raising the "switching costs" across platforms, making each of the platforms a stand-alone silo. This famously frustrated consumers when new devices would emerge that would only work with one particular content protection ecosystem. Microsoft, Google, Apple, and Adobe each had different approaches to the various aspects of DRM, ranging from content protection to policy and trust management. Early attempts to foster interoperability of DRM systems such as the CORAL Consortium and its successors, encountered difficulty overcoming the commercial dissonance from the different stakeholders.

Open standard

Over time, an approach emerged that allows a more unified path to DRM—interoperable in parts—while incorporating siloed technologies, especially the native playback mechanisms. Marlin, an open standard founded by Intertrust Technologies, Panasonic Corporation, Royal Philips Electronics, Samsung Electronics and Sony Corporation in 2005, provides technology for each of the various components, allowing any entity in the distribution value chain to adopt the technology:

- An affiliated trust management organization—Marlin Trust Management Organization (MTMO)—provides credentials and policy templates to the service and device client technology adopters.
- The Marlin Development Community (MDC) developed a series of specifications for DRM that was licensed through the MTMO. Anyone can join the MDC and participate in the development of the specifications and/or make contributions. The specifications were built on the following two major technology components provided by Intertrust:
  - Networked Environment for Media Orchestration (NEMO[1]) provides trust management capabilities
  - Octopus[2] provides the means for coordinating content key distribution with policy management or rules of use for the content
- These are openly published peer reviewed technologies that have proven themselves over a decade of use. The MTMO also provides a set of agreements among the principal content distribution stakeholders: content service providers, device and client providers, and trust service providers. A set of robustness rules are included to ensure that the various key and credential protection mechanisms are implemented in ways that resist attack.

Siloed approaches have been effective for the business models they were designed to support, but the open standard approach has been more broadly impactful, allowing various adopters to use the standard technology components to address new challenges in content distribution. Examples include national initiatives in Japan (IPTV-ES), the UK (YouView), and Italy (Tivú), where a combination of marketing organizations, service providers, content providers, and device providers cooperate to provide protected content to consumers under commercially sustainable models. In these cases, the Marlin specifications were used, but additional trust management capabilities were also applied to allow the identification of trusted components that are part of the system. Today, Marlin is the most widely deployed DRM in China; and in all, there is a growing base of more than two billion Marlin-enabled devices in the global market.

What's next?

Intertrust Research

Intertrust is investing continuously in R&D targeting key management and other system components to make systems much stronger and more scalable. As DRM becomes more robust, we can use DRM for increasingly challenging applications such as protecting live OTT sports streaming.

Some of the potential improvements do not actually involve technology vetting, but rather better coordination among members of the ecosystem. This includes the expanded use of diversity and renewability, both of which would challenge the leverage of an attacker. When an attacker succeeds in undermining the system and obtaining free content, they can illicitly redistribute that content and cause substantial economic harm. But if the protection mechanisms are constantly renewed, and diverse implementations of it are available at any given time, attackers will be frustrated because their specific attack will not be implementable across a portion of the content market sizeable enough to make it a worthwhile action. It may also require that the attacker design, distribute, and maintain their own distribution and playback mechanisms—an investment that may prove untenable.

By reducing a prospective attacker's return on investment, we decrease the motivation to attempt it. This approach applies to professional as well as amateur pirates, who when frustrated by rapid renewability and diversity limiting the results of their conquest, will realize that it is no longer worthwhile.

Even as renewability and diversity are used by DRM and content protection systems, other technologies may get in the way such as policies on distribution of apps in app stores, so better coordination of technology deployment can help.

Intertrust Innovation

Intertrust's position at the forefront of DRM technology development is bolstered not only by its engineering talent, but also by its strategic vision. The Intertrust ExpressPlay suite gives content distributors, network operators, and broadcasters all of the media monetization tools they require in a highly cost-effective and efficient solution.

Trusted by the Biggest Studios

ExpressPlay offers hardware security that meets Hollywood standards for premium UHD/4K and early release window content. All Hollywood studios approve Marlin DRM as a top-quality DRM system and readily license Marlin-enabled services and devices.

ExpressPlay

Intertrust ExpressPlay DRM™

The Intertrust ExpressPlay cloud-based DRM service provides complete, end-to-end protection—device credentials, content key storage, content encryption, multi-DRM license delivery, and secure playback—that meets even the toughest Hollywood standards. ExpressPlay is the only multi-DRM technology available across all popular platforms and formats. Intertrust's service is cost-effective, easy to integrate, and very scalable with a highly available cloud platform.

Intertrust ExpressPlay XCA™

ExpressPlay XCA is a revolutionary card-less content management solution for broadcasters with support for both DVB broadcast-only devices, as well as broadband or hybrid devices. It seamlessly bridges the Conditional Access and DRM worlds. ExpressPlay XCA implements traditional broadcast conditional access system (CAS) rule sets with reliable DRM technology at a fraction of the cost of legacy CAS products. ExpressPlay XCA uses the same content protection engine as the Marlin DRM system, enabling operators to service both broadband and broadcast devices with the same content protection software. Intertrust's use of open standards technology means that ExpressPlay is both flexible and future-proof, freeing customers of proprietary products.

Conclusion

DRM protects content while allowing it to be used according to various rules and policies. There are a number of essential logical components: content protection, trust management, usage and policy management, and robustness technologies. They must be expertly architected into systems that allow the legitimate, free flow of content through distribution channels and onto consumer devices, delivering the intended user experience without a hitch. Most importantly, as much as the state-of-the-art of DRM has provided elegant solutions to current challenges, constant advances in computing power, network designs, and business models requires that DRM technology continues to evolve.

References

1 The NEMO P2P Service Orchestration Framework. Proceedings of the 37th Hawaii International Conference on System Sciences, January, 2004.

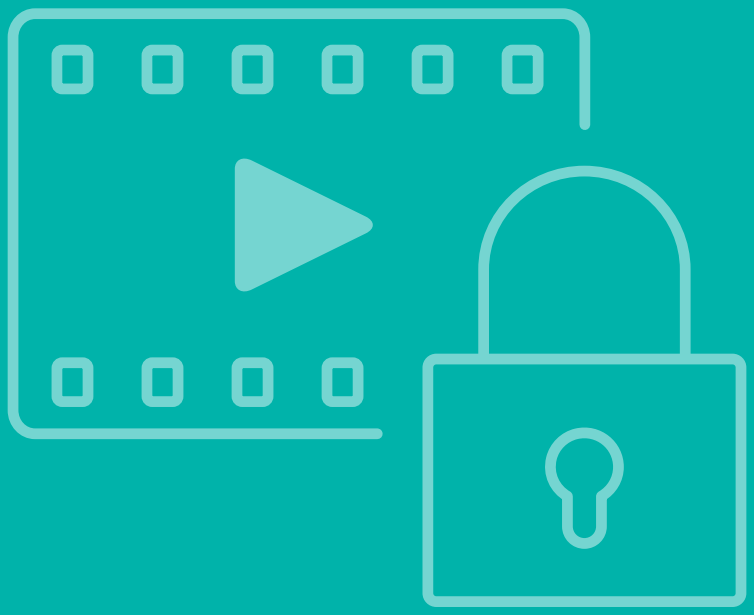
2 Octopus: An Application Independent DRM Toolkit. Proceedings of the IEEE Consumer Communications and Networking Conference, February, 2009.

About Intertrust

Intertrust Technologies is a global technology company with products that are uniquely suited to today's distributed computing environments. From IoT to the cloud, our products ensure the security, privacy, and policy enforcement required for trusted data governance.

As a provider of robust multi-DRM services for media and entertainment companies, our security technology protects the content delivered to any screen and OS platform, over any network.

Intertrust ExpressPlay is the world's most complete multi-DRM security-as-a-service, enabling converged protection for broadcast television and over-the-top (OTT) streaming services.



intertrust®

Building trust for the connected world.

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

Intertrust Technologies Corporation
920 Stewart Drive, Sunnyvale, CA 94085