Digital video broadcasting module

DIGITAL RIGHT MANAGEMENT (DRM)

h.shirazi@qmul.ac.uk

Dr Hamid Shirazi

Table of Contents

Week3: Day-4

Digital Right Management (DRM) Galaxy

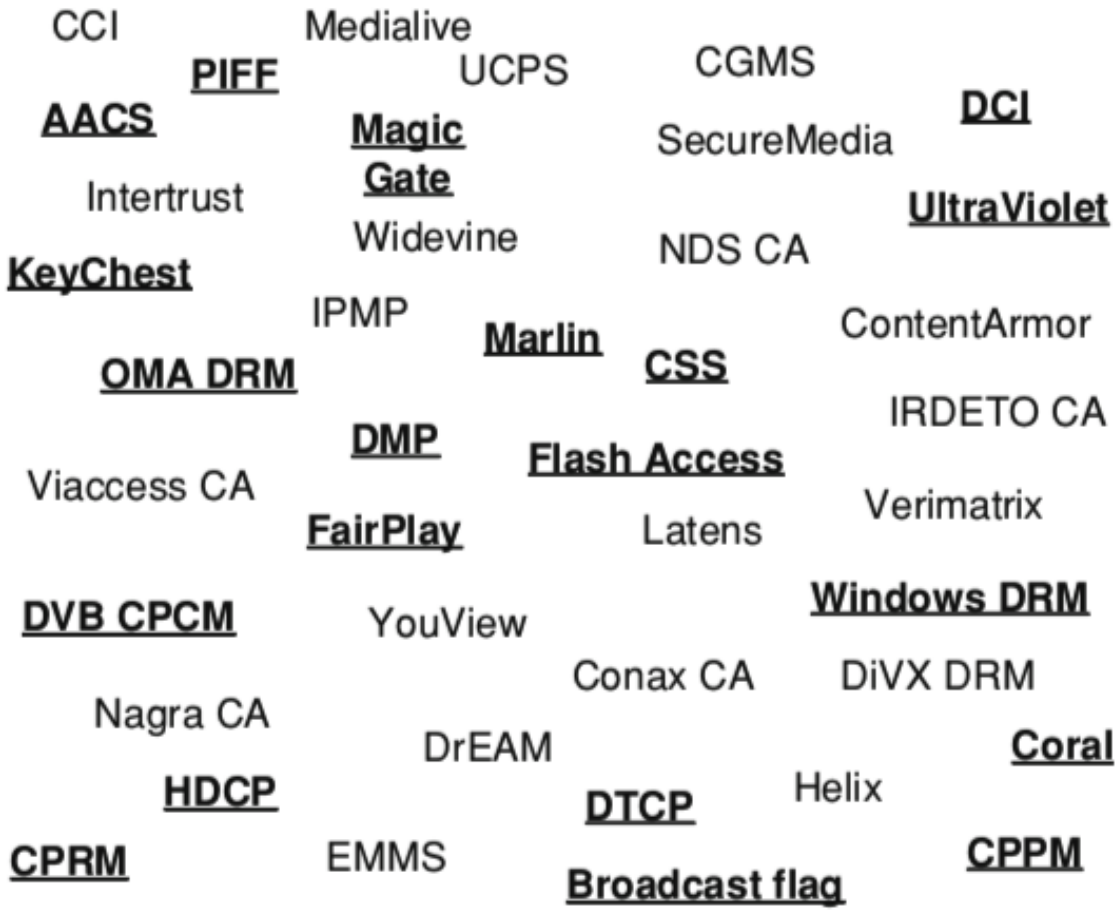


Figure 1: Galaxy of content protection

- UCPS is the Chinese equivalent of HDCP.
- CONAX, IRDETO, NAGRA, NDS, and VIACCESS are conditional access system providers.
- IPMP is a framework for DRM in MPEG4 and MPEG21, which has not been deployed.
- ContentArmor is a professional DRM for B2B developed by Technicolor.
- EMMS, Helix, Intertrust, and Latens are DRM technology providers.
- YouView is the content protection framework of the BBC

Why Content (video) Protection?

- Digital video are fundamentally bits which can be copied, transferred easily or stored.
- Content protection or **Digital Right Management (DRM)** is a broad topic with wide audiences ranging from content producers, service providers, consumer, etc.
- A successful content protection mechanism should address three main areas:
    - **Business model**: recognising consumers' interest in privacy, anonyminty and transferability
    - **Legal constraints**: copy right laws are complex and not universal
    - **Technology**: with limitations it can't always match business and legal requirements

- Copy right laws:
    - Copyright laws give to a creator the **monopoly of exclusive control** of any form of performance and reproduction of his work. Performance means the action of publicly exhibiting any form of the opus, whereas reproduction means duplicating the opus on a physical or electronic medium. Copyright or intellectual property laws define the rules under which contributive works must be rewarded
    - First copy right law is attributed to **English Queen Anne** with statute of Queen Anne in 1710, Apri 10th. In 1952, the symbol © was created and 1996 WIPO (world international property organisation) established a new international treaty, the **WIPO Copy Right Treaty** (but it is only a loose framework and there is no universal copy right law).
    - **Hence, video protection should adapt to each country's local requirements.**

    ❖ Why protection?
    - Laws should protect the interest of the author giving incentive (financially and reputation) for creation and investment in content creation.
    - Laws should protect the investors (e.g. producers and editors)
    - Laws should protect the public interests (e.g. cultural goods) hence rights are valid for fixed a period of time and then it enters publical domain

    ❖ What is Pricay? General rule exists but there are exceptions (fair use)

(1) Contracting Parties shall provide adequate and effective legal remedies against any person **knowingly** performing any of the following acts knowing, or with respect to civil remedies having reasonable grounds to know, that it will induce, enable, facilitate or conceal an **infringement of any right** covered by this Treaty or the Berne Convention:
(i) to **remove or alter** any digital rights management information **without authority**;
(ii) to **distribute, import for distribution**, broadcast or communicate to the public, **without authority**, **works or copies** of works **knowing** that digital rights management information has been removed or altered without authority.

Digital Piracy and Protection Tools

- Digital goods are **non-rivalrous** and **non-excludable** essentially.
    - Non-rivlrous means consumption of goods does not limit its consumptions (e.g. reading books)
    - Non-excludability means prevention of consumption is impossible (e.g. air)
- Piracy types (illegal distribution channel is called **Scene** or **Darknet**)
    - Physical piracy: bootleg CDs or DVDs
    - Digital piracy: P2P networks (e.g. OMEMO), Direct Download (DDL)
- 60% of the pirate copies found in Darknet was due to insiders !
- Warez – groups of crackers (0-day warez[1] or negative-day warez)

- **Video protection techniques** are technological tools that enforce excludability of informaiton goods which otherwise would be public goods creating scarcity of the digital contents (commercial value) → **sequential and separate releases (versioning)**
- **Conditional access** could be one versioning tool to provide a predefined set of utiities for each content for different price tags → studio prespective (business plan)
    - publishing phases start from theatrical realse and continues to airline/hotels, home/rental, VoD/PPV, PayTV, CTV, Syndication, etc.
    - This strategy mitigates second types of piracy (unauthorised distribution)

Case study:

''**Star Trek**'' as an example. ''Star Trek'' was simultaneously available in theaters in selected countries on 6 May 2009. Two days later, the movie was officially released worldwide. The first bootleg DVD hit the street on 8 May 2009. It was a reasonably fair quality camcorder capture coming from a Russian theater. Release teams quickly inter- nationally dubbed this Russian version. Five other camcorder captures appeared, by order of appearance on the Internet, from the Philippines, Ukraine, Spain, Germany, and the US. The Ukrainian copy was of excellent quality and soon became the reference material. At the end of August, more than five million IP addresses downloaded it from P2P sites. There is no estimate of the number of downloads coming from DDL streaming sites. At the same time, 35 million viewers watched ''Star Trek'' in theaters

[1] Same day as official release

A Tool Box – Different Needs Different Tools

- Controlling the access (pysical and logical access – IT security)
    - Only authorised users should be authorised near the asset
    - Business to business relationships, postproduction facilities, broadcast studios are all subect to the access control either by badges or firewalls, etc.
- Protecting the asset against theft, alteration, and replacement
    - Encryption (for confidentiality)
    - Cryptographic signatures (for integrity) plus key management
    - Cryptography is a solution to turn digital content, which is normally non-rival, into a rival good
- Forensic marking if encryption fails provides information about the rendering source.
    - Watermarking is the dedicated technology to perform forensic marking.
    - Forensic technologies can turn digital content, which is normally non-excludable, into an excludable good and provide admissible evidence in the court.
- Preventing illegal distribution:
    - Content can always leak, so losses should be limited by early detection.
    - Fingerprinting is the most effective technique to detect illegal content.
        - A referece database which stores unique characteristics of content e.g. such as visual hashes, color information, time characteristics and points of interests.
        - It is superior to crypto-hash values since it is robust against geometrical modifications, mash-ups and camcorders

Purposes of Cryptography

typical scenario:

Alice and **Bob** are very talkative persons. They always exchange messages. They attempt to have secure transfer, i.e., that their messages cannot be under- stood by anybody other than themselves and nobody can modify these messages.
Eve wishes to learn what Alice and Bob exchange. Thus, she is always eavesdropping on them. She is a passive attacker.
Charlie also wants to learn what Alice and Bob exchange. He is an active attacker compared to Eve.

- Cryptography serves following purposes:
  - Data confidentiality: using secret encryption/decryption keys so that only key holder can understand messages:
    - Algorithms and secret keys are important (without knowing keys decrypting should be almost impossible)
    - Two types of algorithms:
      - Assymetric (public, private keys)
        → signing the hashed messages
          - e.g. RSA (2048bits key) for encryptiion + signature
      - Symetric (ssame key)
        → $c = E_{\{k\}}(m)$ where k: key, m: plaintext
          - e.g. DES (56bit key) and AES (128 or 192 or 256bit key)
  - Authenticity: rightful principal receives the information. It can be secured by a number of secrets.
    - Username/password
    - Token or physical key or smart card
    - Biometrics or user behaviour
  - Integrity: messages are received intact with no modification by e.g. cryptographic hash functions
- HMAC (keyed hash message authentication code) satisfies both integrity and authenticity. It is a secure method of transferring MAC (message authenticate code) which is used to verify the authenticity of the sender
  - The most secure hash algorith is Keccak or SHA-3[2]
  - The most popular is HMAC-MD5

[2] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

Some Observations and Hybrid approach

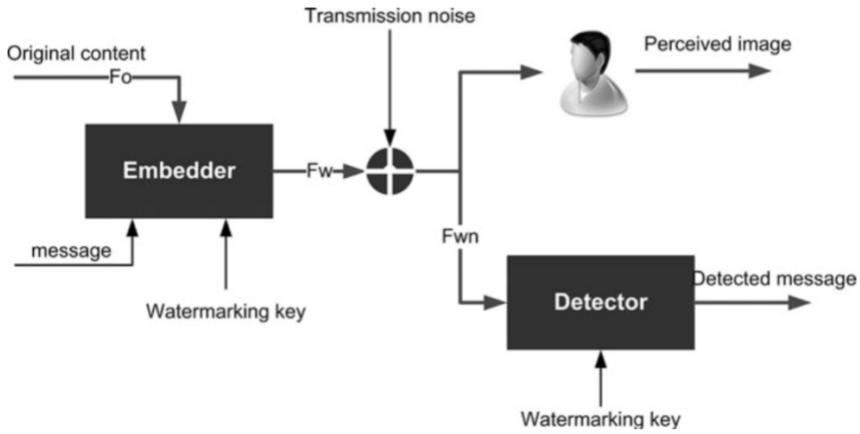
- Symmetric cryptography is fast and suitable for large data sets whereas assymetric cryptography is much slower
    - Symmetric is at least 100 times faster
    - Assymetric is not suitable for large messages
- However, key management in symmetric cryptography is a setback:
    - A population of n people would require n(n-1)/2 shared keys
    - Assymetric resolves this issue by using the (private,public) key pairs
        - Private key remains with sender and public key is stored in a certified directory of keys
            - Hence n people needs only n pair keys
        - A solution is to use session key by the sender, encrypted by receiver's public key which can only be decrypted by receiver's private key
            - Hence both parties will be using same session key and then they can apply symmetric cryptography on the large messages
- Authentication is still an issue – sender and receiver can't identify each other (eavesdropping attack), solution is:
    - To use a known Trusted Third party e.g. Certificate Authority (CA) to link public key to the identity of principal owning the key pair
    - To use a Key certificate is digital information contains following elements:
        - Public key
        - Identity of the owner of the key
        - Identity of the issue of the certificate (CA)
        - Signature of the certificate by CA

        ➢ Hence:
        - Signature will be verified by CA public key (root key)
        - Certificates are usually valid over a fixed period of time (check the expiry date of the certificate)
    - What happens if private key is lost?
        - Public key should be revoked
        - Certification Revocation List (CRL) maintains the most updated records of the revoced public keys

        ❖ Checks must be carried out to ensure CRL is the most recent one and certificate has not been revoked

Watermarking

- Theory:
  - Embedding an imperceptible message into a host multimedia signal without introducing perceptual distortions
  - Message m will be embedded in frame f_0 resulted in modified frame f_w that carries the message m.
  - Watermarking key is essential for the security and is used to randomly hide the message i.e. in a deterministic way that cannot be reproduced without the knowledge of key
    - Embedding the message in the Least Significant Bit (LSB) of Luminance pixel value selected randomly by Pseudo-Random Binary Sequencer (PRBS)



- Usage related to DRM and content protection:
  - Forensic marking: use of watermark to trace the infringer (see next page)
  - Copy Control
    - Receiver should check the watermark for the following signals:
      - Copy never: there should be no copy of this piece of content.
      - Copy once: one generation of copy is allowed, but not more.
      - Copy no more: it is the result of the copy of a ‘‘copy once’’ marked content. It should not be further duplicated.
      - Copy free: the piece of content can be copied without any restriction.
  - Copyright signaling (management)
    - Watermark traces back to the original author or the rights holder (different from forensic marking)
    - It will contain some Information related to copyright and that the content is protected by copyright.
  - Monitoring, monetization: surveying the consumption of a piece of content
    - Embedding watermark to the program (CRID, Channel ID, network ID, time)

Forensic Marking

- To pinpoint the source of potential content leakage in a distribution network
- Forensic marking needs two elements:
    - Using **traitor tracing code** to uniquely identify the component of the network
    - Binding technology (**watermarking)** to bind the content with the issuer
- Potential leakage scenarios:
    - Movie screeners:
        - e.g. leakage of work in progress copy of “The Hulk” in P2P before theatrical release !
        - Solution: embed the watermark (fast and robust) to identify the recipient of a screener
    - In-house tracing:
        - E.g. leakage during the processing of the movie
        - Solution: embed processing stage informaiton (production, post-prod) to trace at which stage the leakage happened
        - Watermarks must take into account quality (fidelity), complete watermarks, and robustness to the post-processing transformations
    - Digital cineman (capturing via camcorder)
        - Embedding a forensic mark just before projection to carry the time, date, video server identity, and location of the projection.
        - The solution must be robust to camcording, realtime embedding and never impair the quality (fidelity)
    - Business-to-consumer: to watermark video output by consumer devices
        - There are two potential architectures:
            - Server side:
                - watermark will be embedded by content server side
            - Client side:
                - watermark will be embedded at the application client side

Business-to-Consumer Architecture Options

- Server side architecture:
    - unique payload is defined by the license server and the content server embeds the watermark before scrambling the content.
    - analysis:
        - it is transparent to the client application
        - it is unique for each client hence multicasting is not supported
        - it is faily secure consider the server side operation but introduced real-time and computational constraints on the content server
        - both computational and bandwidth demanding
        - it is not compatible with pre-srambled VoD approach → unless, restricting watermarking to some parts of the content which are stored clear in the file server
- Client side architecture:
    - at rendering, the unique payload must be embedded by the client application using a unique application ID or license sever to place the payload in the license
    - analysis:
        - Security depends on the client application (software tamper-resistance)
            - Attacking scenario:
                - By passing the watermarking process and issue watermark-free content
                - Modifying the payload hence framing an innocent user
        - It supports multicasting
        - Less resistant to hostile adversaries. Thus, it may face some problems regarding non-repudiability in court.

The trust model of forensic marking is relatively strong.

It assumes that the average pirate has access neither to the embedder nor to the detector. Only employees in charge of marking the screeners should normally have access to the embedder. Moreover, only trusted employees should have access to the detector for investigation purpose.

Therefore, it is reasonable to assume that the pirate will operate blindly.

The objective of the pirate is either to **remove the embedded watermark** to avoid being traced or **modify the embedded watermark** so that an innocent is traced, or to void it.

If a pirate applies a transformation to a piece of content, she has no means to assess whether the attack was successful or not. In other words, she is not certain of not being traced. Thus, to be relatively safe, the pirate has to make extremely strong modifications that severely degrade the quality of the piece of content, making it less valuable.

Hardware Tamper Resistant

- It is set of technologies that make a hardware component such as a processor or memory resistant to **physical** and **logical** attacks
- A secure component should have the following characteristics[3] to be considered as a trusted environment :
    - Participates in electronic transactions: physical attack (opening the case) is trivial
    - Primary purpose of the component is security
    - Difficult to modify and reproduce
    - Stores data in a secure way: so no way to read data through API or microprobing
    - Executes security oriented functions e.g. crypto algorithms.
- There are four types of components that use tamper-resistant hardware:
    - **Secure processors** comes as packaged chip soldered on printing boards or embossed into smart cards (read more: foundation of future smart cards[4] and first commercial use of smart card[5]).
    - There are two types of **smart cards**:
        - Contact cards with 8-pin connector (ISO 7816)
        - Contact-less cards with wireless to receive power, clock and to exchange data
            - Closed-coupled cards (up to 1m range, data rate 9.6kbps)
            - Proximity cards (up to 20cm, 106-817 kbps) – most popular
            - Vicinity cards (10-70cm, a few kbps)
        - Size and power consumption limitations (implying also slow clocks) lead to reduced computing power
            - far less powerful in terms of performance than the usual processors used in computers.
    - Hardware security module (HSM)
        - for key management and comes as PC extension cards which comes with co-processor for cryptographic purposes (assymetric crypto)
    - Security on Chip (SoC) with lots of features including security feature, mainly used in **conditional access systems**, **set-top box** and gateways
        - Modern STB use such chips that integrates a generic main processor (such as ARM, ST, and Atom), a video processor that decodes and renders video signals, and an audio processor. Some chips integrate dedicated video descramblers that support CAS.
    - Trusted platform module (TPM) are secure processors whose unique purpose is to build a trusted environment for a system
        - reliable and secure bootstrap architecture[6]

---

[3] Markantonakis K, Mayes K (2008) Smart cards, tokens, security and applications. Springer, Heidelberg

[4] Moreno R (1976) Methods of data storage and data storage systems. US Patent 3,971,916, 27 July 1976

[5] http://www. aconit.org/histoire/colloques/colloque2004/guillou.pdf

[6] Arbaugh WA, Farber DJ, Smith JM (1997) A secure and reliable bootstrap architecture. Proceedings of the IEEE symposium on security and privacy, Oakland, CA, USA, pp 65–71

Software Tamper Resistant

- Securing software is a difficult, if not impossible, task. This is especially true in the case of DRM, where only a few elements can be trusted.
    - Realistically, tamper resistant software is **just a barrier** to entry for attackers
- Tamper resistant software for DRM typically has three **objectives**:
    - code **integrity** as well as execution integrity:
        - to ensure that the DRM client protects itself against tampering by a malicious host;
    - code **privacy**:
        - to ensure that the DRM client can conceal the program it wants executed on the host
    - key **secrecy**: security of secret keys so that they must not be revealed to the host:
        - to ensure that the DRM client can decrypt information without disclosing the corresponding decryption key.
- 4-Phase scenario of attacking:

  Analysis (data grathering) → Tampering → Automation → Distribution
- Some recommendations to software engineers:
    - Minimize the collected data
    - Make reverse-engineering difficult
    - Detect or, better, prevent tampering
    - If the software is tampered with, either repair it or act in a defined way such as stopping, degrading behavior, and alerting a remote site
    - Prevent repeatable hacking; the scope of the hack should be limited at best
    - **The worst case is a hack that affects all the deployed systems. In this case, the hack is called a class attack**

Software tamper-resistance is based on security by obscurity

Rights Expression Language (REL)

- Rights Expression Languages (REL) describe the **usage rights** of a protected piece of content
- REL must have the following characteristics:
    - It must be machine-readable because it has to be translated by the DRM agent.
    - It must be expressive enough to support the requirements of the content owners, service providers, and merchants.
    - It must be formal and unambiguous. It must be able to translate from com-
    - mercial rights into usage rights enforced by DRM and vice versa.
- Commercial rights are expressed in natural languages
    - e.g. ''a monthly subscription to ''Syfy'' channel''
- Translating usage rights to commercial terms (license):
    - The license describes the agreements between the party that grants the rights (issuer) and the party that receives these granted rights (subject) over an object.
        - Rights of e.g. ''print'', ''view'', ''edit'', ''copy'', or ''transfer'', etc.

Four Layer Content Protection Model

- It is a layered model which describes the security of a DRM or a content protection system through four main features:
    - Content protection:
        - typical technique is encryption (scrambling) of content using encryption (secret) key and scrambling algorithm or
        - altering the content using visible or invisible techniques for forensic marking e.g. logo, watermark
    - Rights enforcement:
        - protecting usage rights and encure they are complied with by provisioning of encryption key to client
        - @server side: encapsulating usage rights defined by rights management layer, secret key and some other data which together form license or Entitlement Control Message (ECM)
            - ECM will be signed and encrypted
        - @client side: ECM signature and together with rights management layer verifies if client is authorised, if so, secret key will be provided to content protection
    - Rights management
        - Handles usage rights associated with a piece of content
        - Translates commercial rights to usage rights and forwards them to rights enforcement layer
    - Trust management:
        - It ensures that only trustful principals interact:
        - It ensures that each principal is what it claims to be, and that it is authorized to participate in the system.
        - It ensures that each principal of the system behaves as expected.
- Figure 2 illustrates the interactions between layers.

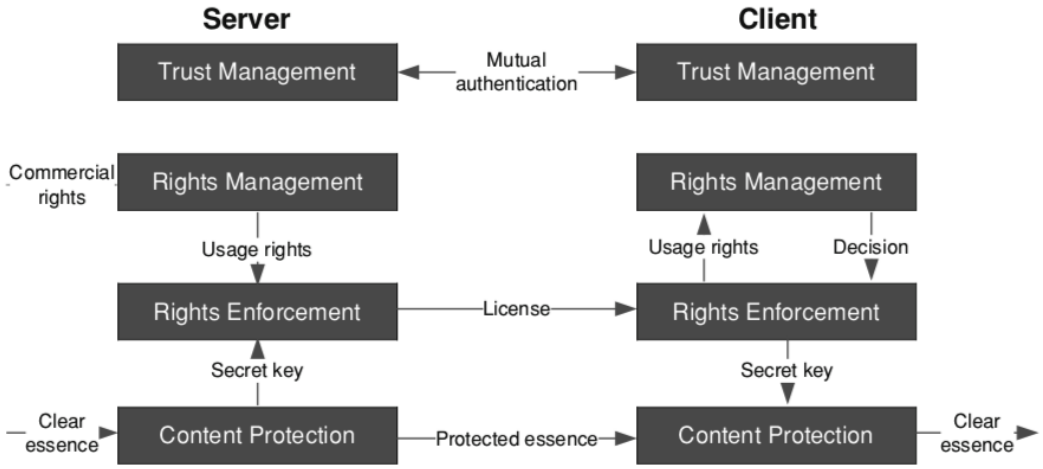


Figure 2: interaction between layers

Content Delivery and Business Models

- Content delivery modes:
  - Broadcast channels (DVB-S/C/T):
    - One way channels and implies that same program will be transmitted simultaneously to every viewer and there is no return channel.
  - Unicast/multicast channels (IP connections):
    - Unicast is delivery to a unique address and multicast is delivery to multicast group (set of IP addresses) receiving via modem gateways
    - Distribution methods:
      - Network Service Provider (NSP) or Internet Service Provider (ISP) commercial offers
        → controlled network hence guaranteed QoS
      - Over The Top (OTT) through normal IP connection (web service)
        → no control over the allocated bandwidth hence difficult to guarantee QoS
    - Distribution channel could be through mobile networks (UMTS, LTE) or Internet connections (broadband)
- Business models:
  - Free to Air (FTA) or Freeview:
    - tuner will receive the signals
    - could be geographically limited (only for national viewers)
      - in satellite, some kind of conditional access could be used
    - broadcasters will pay more for the license (wider audience)
  - Pay-TV channels
    - Only for paying subscribers
    - STB equipped with conditional access system (CAS) is needed

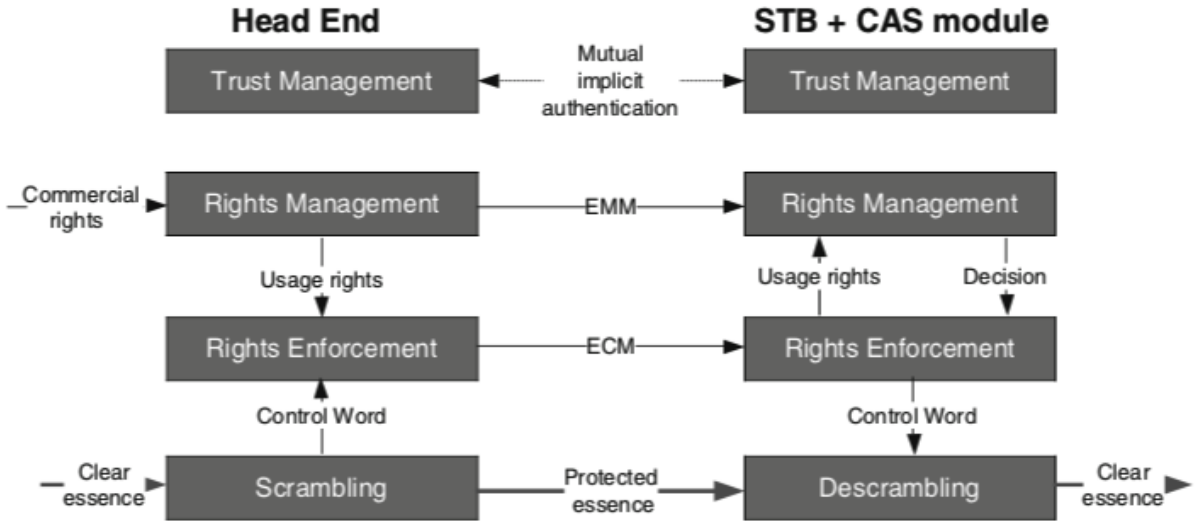
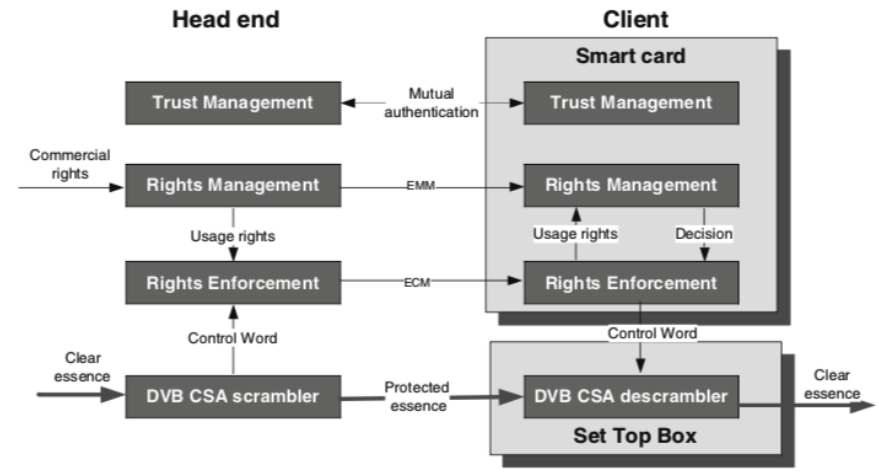


Figure 3: Pay-TV four layer model

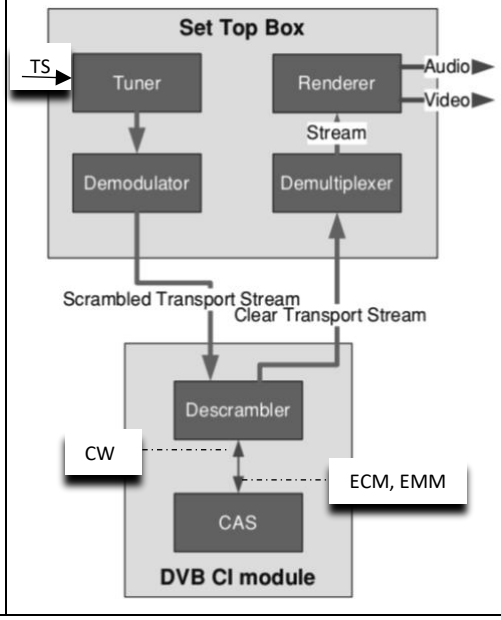
DVB (Broadcasting) Protections

- DVB Common Scrambling Algorithm (DVB-CSA) is used to protect contents
- It uses 40-bit key Contro Word (CW)
- DVB-CSA's crypto period can vary from 10 to 120 s
- Architecture:
    - Each STB has an associated smart card.
    - The smart card hosts the rights enforcement layer, rights management layer, and trust layer, whereas the STB hosts the protection layer.
        - Renewing three upper layer can be done by sending a new smart card
        - Specification and security of smart card is managed by CA provider
          → CAS could be different in the way three layers are managed
        - DVB only specifies the content protection layer, ECMs and EMMs, and the way to carry them within a DVB transport stream.
- DVB-Common Interface (CI) and DVB CI module introduced to support multiple CASs
    - Hence, every part related to Pay-TV is ported into the detachable DVB-CI module. The DVB STB becomes generic and fully independent of CAS flavors.

DVB four layer mode



Architecture of DVB-CI

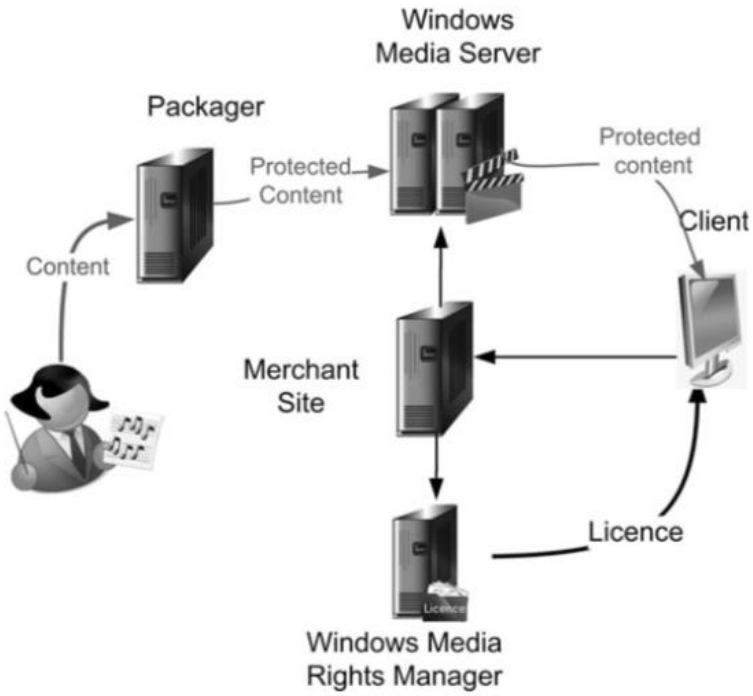


Unicast/Multicast DRM Protections

- DRM usually protects content delivered over broadband connections using unicast and multicast modes.
- Although functionally very similar to CAS, DRM systems have two significant differences:
    - As DRMs have to run on generic computers, they operate in a less trusted environment than does CAS.
    - Their trust model cannot rely on tamper-resistant hardware. Instead, the trust model must rely on software tamper-resistance and easy renewability by forcing the customer to download a new version of the software in the event of a hack.
    - DRM assumes the presence (even temporary) of two-way communication, which enables more flexible license management, and some security controls by the remote server.
- Architectural Model, they all have at least three common elements:
    - a content packager
    - a license server
    - a client DRM.
- It is extremely difficult to find public information describing security features.
- main actors in the field: Microsoft DRM (or PlayReady) and Apple FairPlay and Google Widevine

Microsoft DRM

- Most popular and widely deployed DRM attached to Windows Media Player
- Microsoft WMDRM has four elements:
    - The Packager prepares the piece of content to protect.
        - Appends a header which includes KeyID, Content ID, WMDRM version number (use the most secure version), URL of license server
    - The Windows Media Server stores the packaged piece of content and distributes it to the customer.
    - The Windows Media Rights Manager generates the licenses.
    - The Windows DRM client handles the delivered piece of content and license. If allowed, it delivers or renders the clear piece of content.
        - The client is often hosted in Windows Media Player. Nevertheless, device manufacturers or system integrators may implement the Windows DRM client in their own media player.
- Encryption technique:
    - Symmetric encryption algorithm (AES) using a 128-bit random key.
    - The random key is generated from two pieces of information:
        - License key seed is a secret data only known to the Windows Media Rights Manager and the content owner who delivered the clear content. The license key seed is unique for each piece of content to be protected.
        - Key ID, often referred to as the KID, is public information that is unique for each Windows Media file.
- Since 2008, PlayReady come to the market with less restrictions supporting other OSs and being content agnostic supporting any type of digital contents.

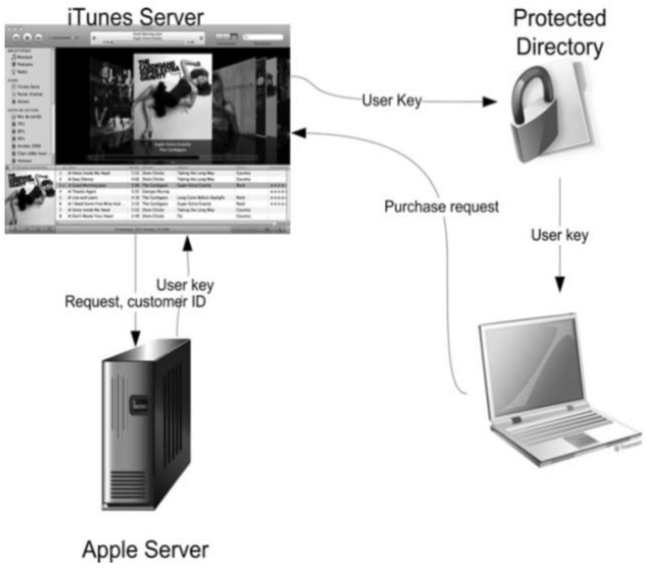
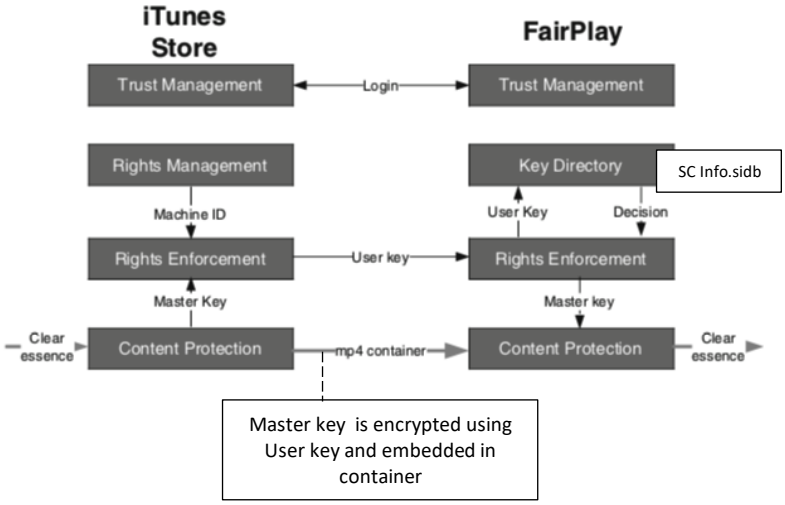


When client finalised the purchase, merchant site orchestrates the delivery of lincese and purchased content through windows right manager andn media server to the client.
License can be deilvered in three ways:
Silent delivery (direct delivery to client), Non-silent deilvery requires acknoledgement from mechant portal, and license pre-delivery which is good for subscription based model and similar to silent deilvery.

Figure 4: Transactional model of WMDRM

Apple Fairplay

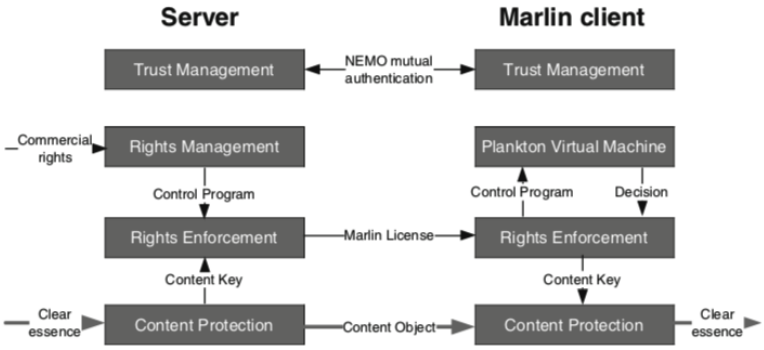
- In January 2001, Apple opened the iTunes store to boost the sales of iPods. For iTunes to be attractive to consumers, it had to offer a large catalog of good songs. Apple had to negotiate with the major studios. DRM was about their main requirements.
    - Apple was not in favor of DRM, Steve Jobs predicted the end of DRM in his famous manifesto[7].
        - It is important to keep in mind that Apple's main business model is the sale of hardware rather than software
        - However, the use of proprietary formats and DRM is an efficient way to lock consumers to the brand's product lines
- Every piece of content is contained in mpeg-4 and scrambled with a master key using AES
- The database is encrypted using a two-step process:
    - The plaintext database is XORed with the output of a proprietary Pseudo- random Number Generator (PRNG) seeded with unique information extracted from the client (e.g. machine ID).
    - Then, it is AES encrypted with one more unique piece of information extracted from the system of the computer.

Transcation model	FairPlay four layermodel
	

[7] Doctorow C (2006) Opinion: Apple's copy protection isn't just bad for consumers, it's bad for business. Information Week, July 2006. http://www.informationweek.com/news/global-cio/showArticle.jhtml?articleID=191000408

Marlin

- Marlin is a DRM dedicated to consumer electronics devices initially designed by Intertrust, Panasonic, Philips, Samsung, and Sony in 2005
- It is based on two frameworks:
    - Octopus[8]:
        - Octopus is a generic engine that protects digital content regardless of the type of content (audio, video, text) and the usage rights.
        - It uses two concepts:
            - Octopus nodes and links.
                - An Octopus node represents a logical entity such as a user, a device, a domain, or a subscription.
                - A link defines a logical relationship between two Octopus nodes.
            - e.g. a link may declare that Octopus personality node A, which represents device A, belongs to Octopus user node Alice.
    - Networked Environment for Media Orchestration (NEMO)[9]:
        - NEMO framework defines the secure communication between the different Marlin entities, the so-called NEMO nodes.
        - A NEMO node is a trusted entity that securely interacts with others NEMO nodes.
        - Goals:
            - Authentication: only trusted nodes can interact with each other
            - Message security: secure communication between nodes enforcing privacy and integrity of the data
            - Authorisation: nodes may require certain properties before communicating (attribute assertions).
            - Service discovery: nodes must be able to locate nodes that may propose needed services.



Marlin four layer model:
Content key is used to scramble the content and bound to personality node.
Control program (executable code) contains associated commercial rights and defines the targeting for the content object and checks if personality node has a set of links that reach the required nodes.
Marlin license holds encrypted ontent key, encrypted control program, and signature of control program (HMAC)

[8] Boccon-Gibod G, Boeuf J, Lacy J (2009) Octopus: an application independent DRM toolkit. Proceedings of the 6th IEEE conference on consumer communications and networking, Las Vegas, NV, USA. IEEE Press, 2009, pp 1148–1154. http://portal.acm.org/ citation.cfm?id=1700527.1700809

[9] NEMO_Specifications.v.1.1.1, 2010. http://www.intertrust.com/system/files/NEMO_ Specifications.v.1.1.1.pdf

Protection with Home (brief)

- The digital home network handles a plurality of devices using different media such as Ethernet, General Packet Radio Service, Wi-Fi, and USB. T
- he home network encompasses fixed devices as well as mobile devices.
- It encompasses consumer electronics (CE) devices as well as personal computers and mobile phones.
- There are four roles in the home network:
    - Acquisition point where a piece of content enters the home network
        - DRM/CAS could be applied
        - If user is entitled, DRM is translated to common protection system (CPS)
        - Interoperability occurs at this point
    - Storage points where contents are stored such as hard drive
        - Link protection e.g. DTCP
        - Contents remain scrambled till rendering points
    - Rendering point where contents are rendered for use by the consumers
        - It can play if it supports media format and CPS
        - It connects to the online server (digital locket) for translation of usage rights
    - Exporting point where contents are transferred to out of home network

Interoperability Challenges

- Consumers expect to have a seamless experience
    - Consumers still expect to play their content on any of their numerous appliances
    - Frustrations:
        - Restricted user experince
        - Old formatted contents are not always supported by new DRMs
        - Incompatibility between multiple DRMs created even by one company
        - Purchased contents are sometimes no longer playable in new devices
- There are many competing DRM solutions and most of them are not interoperable
- Interoperability goals:
    - DRM1 and DRM2 use compatible scrambling formats or convertible formats. This requires interoperability at content protection layer should be compatible:
    - License of DRM1 to be translated into license conforming to DRM2. This requires interoperability at the rights management and rights enforcement layers.
    - DRM1 must be sure that the terminal hosting DRM2 is trusted before handing
    - over protected content. This requires interoperability at the trust management layer.
    - Today, most DRMs do not trust each other ☹
- Different types of interoperability:
    - vertical approach – full format interoperability
        - solves the interoperability issue by defining one universal format and protection scheme used by every device.
    - horizontal approach – partial interoperability
        - solves the interoperability issue by defining some common interfaces and mechanisms while the definition of the remaining elements stays open.
    - plug-in approach – configuration driven interoperability
        - solves the interoperability issue by providing a framework that first locates and then downloads the tools needed to implement the actual DRM.
    - translation approach – connected interoperability
        - solves the interoperability issue by defining a set of mechanisms that convert protected content from one DRM into another DRM.
    - Interoperable Rights Locker – most promising approach
        - solves the interoperability issue by merging the horizontal approach with the translation approach.