2 Digital Rights Management

Literature:

Bill Rosenblatt, Bill Trippe, Stephen Mooney: Digital Rights Management – Business and Technology, M&T Books 2002

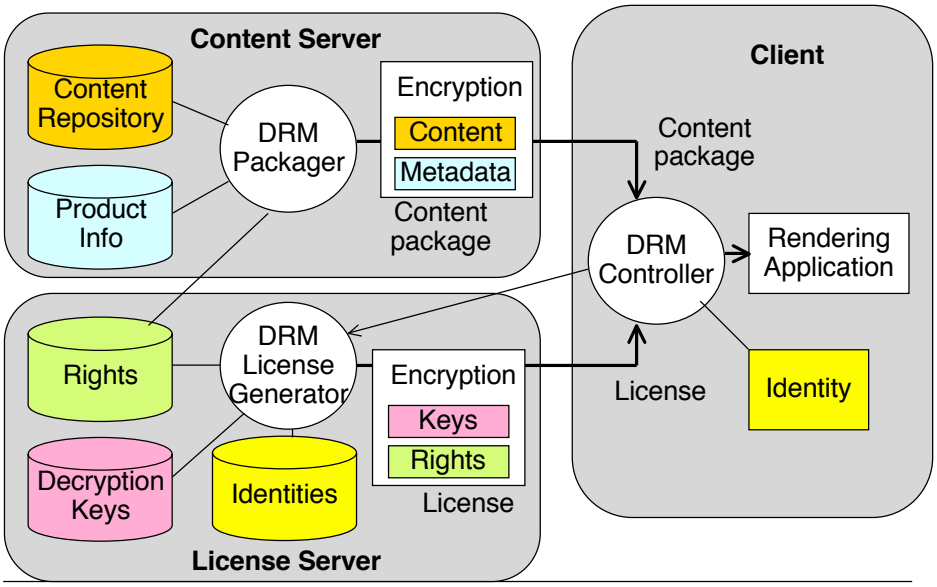
Seth Schoen: Trusted Computing - Promise and Risk, http://www.eff.org/Infrastructure/trusted_computing

Eberhard Becker et al.: Digital Rights Management – Technological, legal and political aspects, Springer 2003 (LNCS 2770)

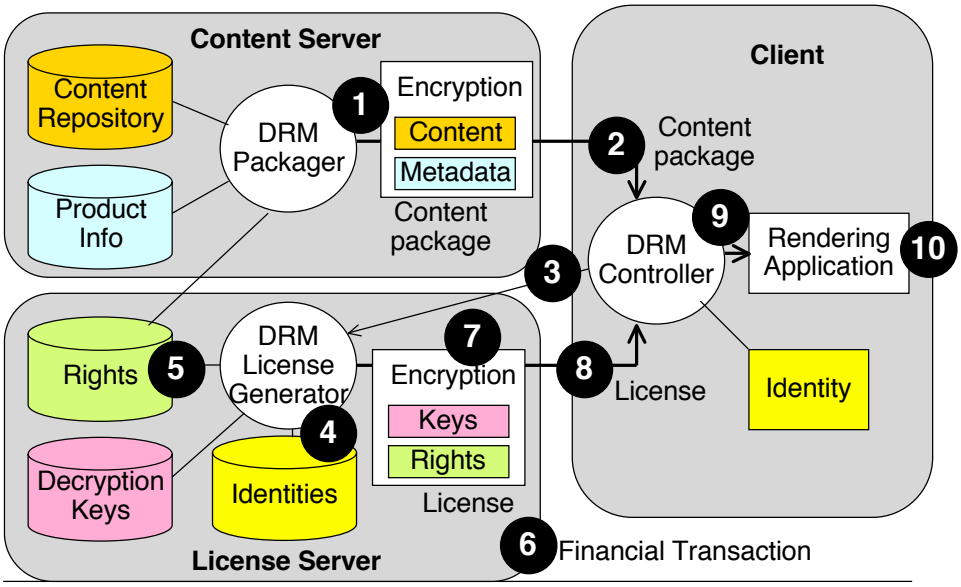
Encryption-Based DRM

- Content is transmitted to users only in *encrypted* form
  - Not readable/playable without decoding using appropriate *keys*
- A *license* contains keys, coupled with *rights*
  - Rights specified according to a rights model
  - Keys have to be inseparable from rights
  - Licenses can and should be separate entities from content files
    - » Different licenses for same content
    - » One license for many pieces of content
- *User identities*
  - Ensure that rights are granted to a specific person or organisation
  - Correspond to the “principals” of XrML
- *Device identities*
  - Ensure that restrictions on device usage are checkable
  - E.g. using some content only on a limited number of devices

A DRM Reference Architecture



10 Steps To Play Protected Content (1)



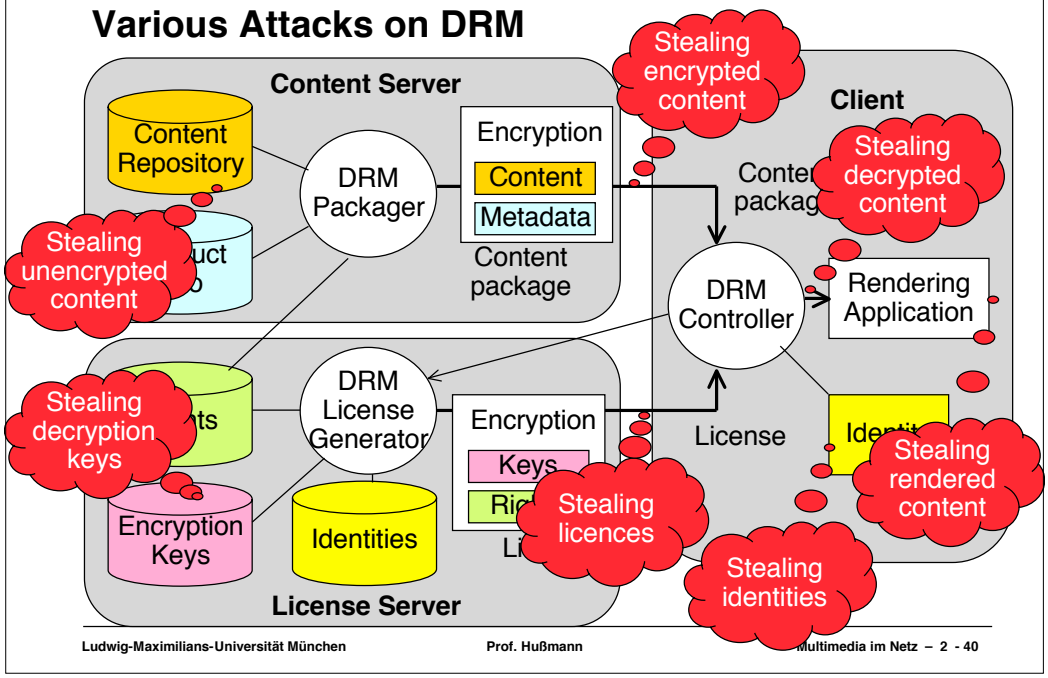
10 Steps To Play Protected Content (2)

- (1) User obtains a content package, e.g. by download
- (2) User makes request to exercise rights, e.g. to play or store the content
  - Rendering software activates the DRM controller
- (3) DRM controller determines identity of user and content and contacts license server
  - May require user interaction, e.g. filling a registration form
- (4) License server authenticates user against identities database
- (5) License server looks up rights specification for the requested content
- (6) If necessary, a financial transaction is started
  - Financial transaction may happen also at another point in the process
- (7) License generator combines rights information, client identity and decryption keys and seals them (packaged by encryption again)
- (8) License is sent to the client
- (9) DRM controller decrypts the content and hands it over to the rendering application
- (10) Content is rendered for the user

Identification

- User identification
  - Supplied by user: User name, password
    - » Can be passed on from user to user
  - Inherent: Biometric data
  - Supplied by trusted third party: Digital certificate
- Device identification
  - Serial number readable by software
    - » Seen problematic by data privacy advocates (cf. Intel's attempts)
  - IP address
    - » Unsuitable, due to techniques like NAT (network address translation)
  - Combination of various identifying information

Various Attacks on DRM



Integration DRM Controller – Rendering

- The coupling between DRM Controller and rendering application has to be very tight
  - Intermediate storage of decoded data in file or socket would be harmful
- DRM Controllers can be built into rendering software if there is enough market (segment) domination of the rendering software
  - E.g. Adobe Acrobat, various eBook readers
  - E.g. Microsoft Windows Media Player, Apple iTunes & QuickTime
- DRM Controllers can be built into specialized devices like portable music players
  - E.g. Apple iPod
- General problem:
  - Decoded digital signal has to be stored and transmitted somewhere in the computer software
  - It will always be possible to capture the decoded signal on hardware or operating system level
    - » Except with “trusted systems”…

Trusted Computing and DRM

- Microsoft initiative: “Palladium” architecture (now named “Next Generation Secure Computing Base (NGSCB)”)
  - Bill Gates: “We came at this thinking about music, but then we realized that e-mail and documents were far more interesting domains.”

    (Quotation according to Rüdiger Weis, cryptolabs)
- “Trusted Computing Platform Alliance” (TCPA), since 2003 called “Trusted Computing Group (TCG)” (https://www.trustedcomputinggroup.org/home)
- Authentication and validation of software and documents built into operating system and based on “tamper-proof” hardware
  - Promises:
    - » (Almost) unbreakable realization of DRM
    - » Complete control over software licensing
    - » Secure storage for sensitive information like electronic money or valuable keys

TPM = Trusted Platform Module

AMD hp invent IBM Infineon intel lenovo Microsoft Sun microsystems

Key Concepts of Trusted Computing

- Memory Curtaining
  - Hardware-enforced memory isolation to prevent programs from reading or writing other program’s memory
  - Excluding even the operating system from accessing curtained memory!
- Secure Input/Output
  - Secure hardware path to and from input/output devices
- Sealed Storage
  - Sensitive information like cryptographic keys is not simply stored but generated if authorized software runs on an authorized machine
  - Encrypted in a way including the identities of the encrypting program and the current hardware
- Remote Attestation
  - Unauthorized changes of software detectable from a remote system (before actually sending data to the suspicious system)

Pros and Cons of Trusted Computing

- Pro:
  - An effective countermeasure against threats by viruses, hackers etc.
  - Helps to ensure privacy and confidentiality of user data
  - Enables interoperability of systems over open networks
  - Respects privacy, keeps user in control
- Contra:
  - Relies much on Trusted Third Parties
  - Can be misused for censorship and customer lock-in
  - Collection and transmission of private data not transparent to users
  - Strengthens monopolies, reduces competition
  - Complicates the situation for open source software
  - Enables restrictive DRM
  - See also:
    - » Ross Anderson: http://www.cl.cam.ac.uk/~rja14/tcpa
    - » Critical movie: http://www.lafkon.net/tc/

2 Digital Rights Management

Literature:

Bill Rosenblatt, Bill Trippe, Stephen Mooney: Digital Rights Management – Business and Technology, M&T Books 2002

Seth Schoen: Trusted Computing - Promise and Risk, http://www.eff.org/Infrastructure/trusted_computing

Eberhard Becker et al.: Digital Rights Management – Technological, legal and political aspects, Springer 2003 (LNCS 2770)

Watermarking

- Watermarks convey information about a document
  - Without interfering with the appearance or readability of the document
  - By being inextricably bound together with the document
- Recognizable watermarks:
  - Clearly recognizable, e.g. logos in video information
- Hidden watermarks:
  - Similar to “Steganography”
    - » Steganographic message: existence usually not expected
    - » Watermark: hidden, but existence usually known
- Watermarks typically carry “metadata” about the document
  - Universal watermarks: Information about copyright, original source, …
  - Individual watermarks: “fingerprinting” of individual copies
    - » Tracing back copyright violations

Characteristics of Digital Watermarks

- Undetectability:
  - The watermark does not detract from the visual or audible experience of the content
- Robustness:
  - The watermark survives copying to lower-resolution formats or from digital to analog formats
  - “Analog hole” = Way around digital copy protection by re-digitizing the analog content
- Capacity:
  - The watermark should be able to contain as much data as possible
- Security:
  - The watermark resists attempts to erase or alter it
- Efficiency:
  - The overhead created by inserting or extracting the watermark is tolerable
- Watermarking cannot prevent unauthorized copying, but can help DRM controllers
  - to determine the source of multimedia information and trigger copy-protection
  - To obey rules encoded in the watermark (e.g. usage time information)

Principle of Watermark Insertion

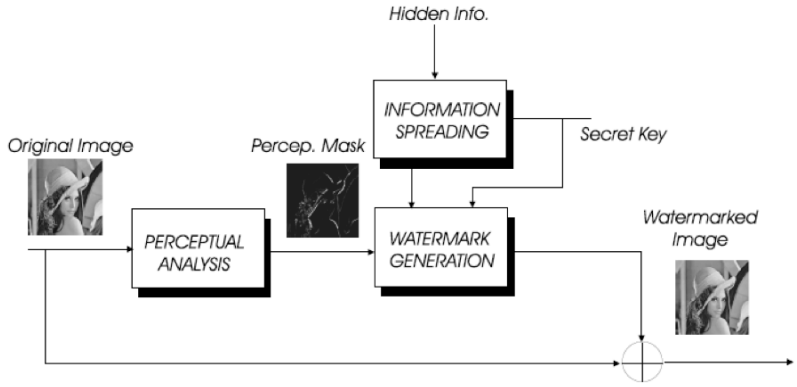


Figure 1: *Watermark insertion unit*

- From: Fernando Perez-Gonzalez and Juan R. Hernandez, A TUTORIAL ON DIGITAL WATERMARKING

Principle of Watermark Extraction

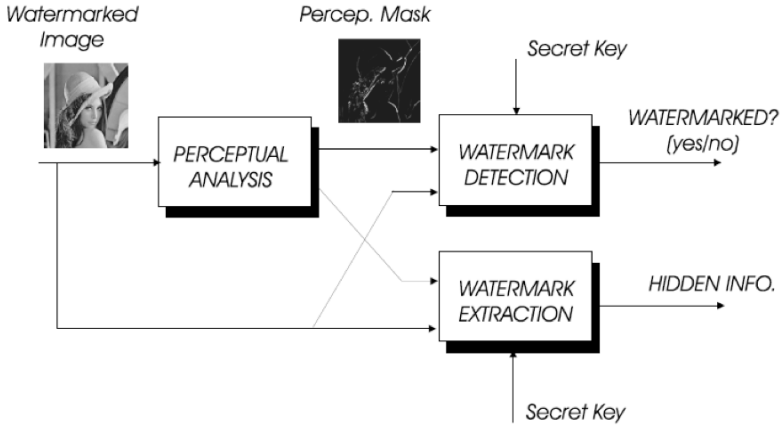


Figure 4: *Watermark detection and extraction unit*

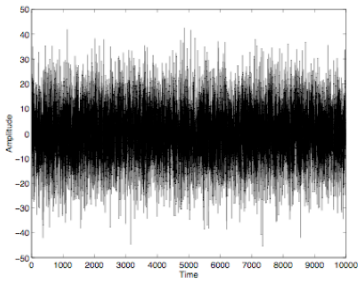
- From: Fernando Perez-Gonzalez and Juan R. Hernandez, A TUTORIAL ON DIGITAL WATERMARKING

Watermarking and Perceptual Significance

- Naive idea:
  - Use parts of the audio/image encoding which are not relevant for user perception, e.g.:
    - » Masked frequencies in audio (e.g. between MP3 truncation threshold and perception threshold)
    - » High frequency AC coefficients in JPEG
    - » Low-significance bits of samples
  - Robustness problem: Easy to remove
- Using a *perceptually significant* part:
  - E.g. Low-frequency parts of audio/image
  - Removing the watermark causes perceptible distortions
  - Undetectability problem: Danger of becoming perceptible

Typical Spread-Spectrum Watermarking

- Spread-spectrum:
  - Signal is spread over more bandwidth than necessary for its encoding
- Spread-spectrum watermark:
  - Encoded in broad frequency spectrum
  - Mid band frequencies (not too high or too low)
- Spreading according to key:
  - E.g. seed for random sequence
  - Secret to be known for extraction
- Sketch of a possible algorithm for images:
  - Select luminance component
  - Map to values representing human perception levels (e.g. logarithmic values)
  - Apply FFT and encode in mid-band coefficients
  - Apply inverse FFT and rescale colour components



Source: O'Ruanaidh/Pereira

Example: DigiMarc Technology

- www.digimarc.com
- Digital watermarking of images and pictorial documents:
  - Geo-spatial data (e.g. satellite images)
    - » Ensuring the integrity of the data, tracking the usage
  - ID documents (e.g. travel passports)
  - Financial documents (e.g. bank notes, financial instruments)
    - » Identifying genuine documents, detecting alterations

Original unwatermarked image | Digimarc watermarked image | Exaggerated view of imperceptible Digimarc watermark

Attacks on Digital Watermarks

- Removal attack
  - Consider watermark as noise and reconstruct original information, e.g. by median filtering
  - Variant: “collusion attack” on fingerprinted content, create mix of versions
- Oracle (or sensitivity) attack
  - Assumes access to a watermark detector
  - First step: Create modified image close to decision threshold of detector
  - Second step: Modify luminance of each pixel until detector switches
    - » Create minimal distortions but keep out of watermark detection
- Stirmark attack:
  - Create small random geometrical distortions (e.g. minimal warping)
  - Modified version is no longer recognized as watermarked by detector
  - Loss of synchronization/correlation in watermark information
- Tendency: Robust watermark technology is extremely challenging

2 Digital Rights Management

Literature:

Bill Rosenblatt, Bill Trippe, Stephen Mooney: Digital Rights Management – Business and Technology, M&T Books 2002

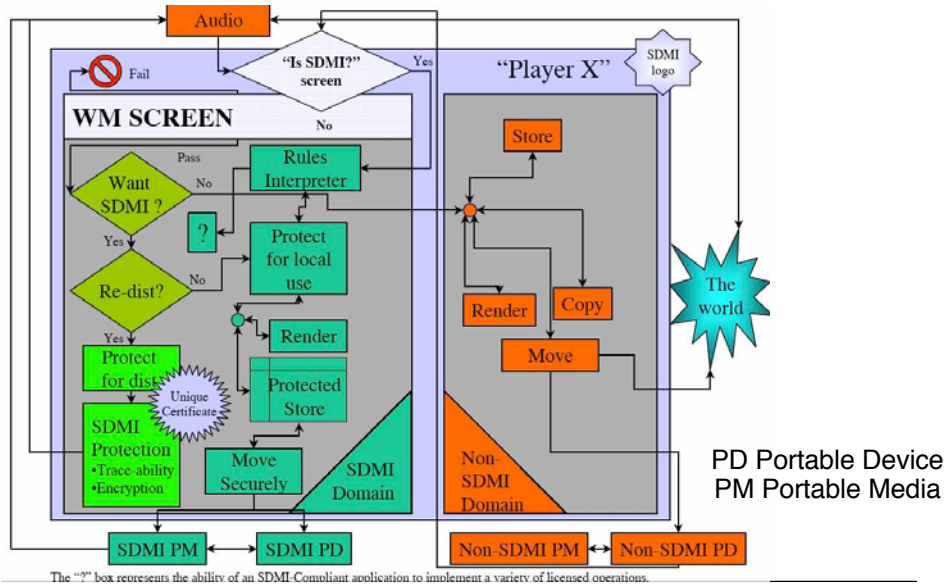
Intellectual Property Identification: DOI

- Digital Object Identifier (DOI)
  - Unique identification of any kind of digital content
  - Initiative started 1994, active ANSI/NISO standard in 2004 (see www.doi.org)
    - » Currently over 20 million DOIs assigned
- Based on IETF “Uniform Resource Identifier” standard
- Syntax:
  `doi: Prefix / Suffix`
- *Prefix* of form **`directoryID . publisherID`**
  - Can be obtained by publisher from a registration agency
  - Currently always starts with “10.” (built for extension)
- *Suffix:*
  - Can be determined by publisher in arbitrary syntax
  - E.g.: **`doi:10.1016/S0167-6423(02)00032-1`**
- DOI directory (http://dx.doi.org/) resolves DOI to a URL
  - Publisher responsible for maintaining the information

Secure Digital Music Initiative SDMI

- 1999: Initiative of music industry: Set of open standards for online distribution of digital music with built-in rights management
  - Recording Industry Association of America (RIAA)
  - “Big 5” record labels (Sony, Warner, BMG, EMI, Universal)
- First goal: Standard for DRM-enabled MP3 players
  - Chartered Leonardo Chiariglione from Telecom Italia (MPEG chair)
  - Result: High-level architecture for a long-term perspective in digital music
    - » Uses watermarking (for copy-protected content playable on other devices) and encryption (for fully protected content playable only on SDMI devices)
  - Plan for a two-phase transition:
    - » In phase I, players play music in any format
    - » When SDMI watermarked content is detected, users are asked to upgrade to a Phase II device

SDMI Licensed Compliant Module Architecture



The SDMI Challenge

- 2000: SDMI technology evaluation for Phase II
  - Open call for proposals from technology vendors
  - Public challenge (“Hack SDMI”)
- Team from Princeton University around Edward Felten:
  - Successfully cracked most of the proposed technologies and was confident of being able to crack all
  - RIAA prohibited publication of paper on these results (Information Hiding Workshop, February 2001), using legal measures based on DMCA
  - After heavy media coverage, paper finally was presented at USENIX symposium (August 2001)
- Current status (from www.sdmi.org):
  - “Based on all of the factors considered by the SDMI plenary, it was determined that there is not yet consensus for adoption of any combination of the proposed technologies. Accordingly, as of May 18, 2001 SDMI is on hiatus, and intends to re-assess technological advances at some later date.”

MPEG-21

- “Normative open framework for multimedia delivery and consumption for use by all the players in the delivery and consumption chain”
  - www.chiariglione.org/mpeg/standards/mpeg-21/mpeg-21.htm
  - Currently (2006) still under construction
- Users: Covers content providers and consumers
  - In principle, all operations on content available to all users
- Digital Item:
  - Definition non-trivial for dynamically changing content (e.g. scripting)
  - Precisely defined in MPEG-21 Part 2: Digital Item Declaration (DID)
  - Identification and classification of Digital Items (MPEG-21 Part 3)
- Intellectual Property Management and Protection (IPMP)
  - Interoperable framework for IPMP defined in MPEG-21 Part 4
  - Rights Expression Language (REL) defined in MPEG-21 Part 5
    - » Mainly based on XrML
  - Rights Data Dictionary (RDD) defined in MPEG-21 Part 6
    - » Mainly based on <indecs>

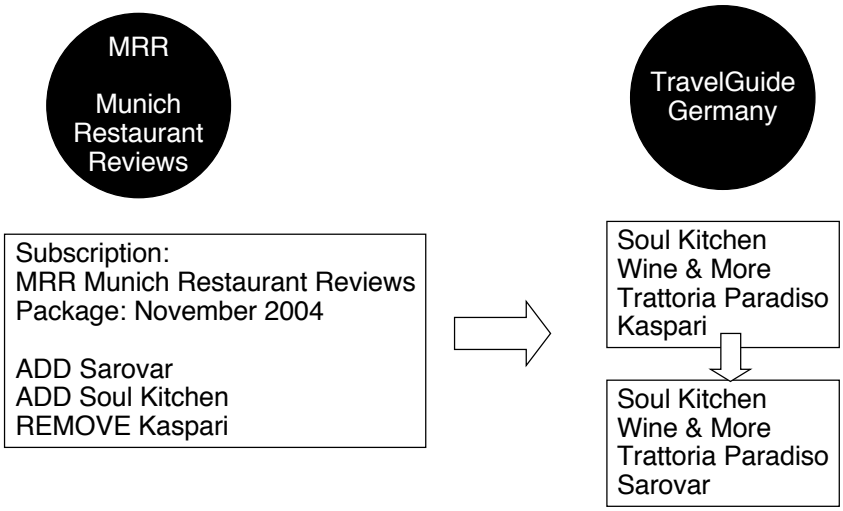
Rights Data Dictionary (RDD)

- Rights Management Systems differ in their terminology schemes
- Rights management is often combined with terminologies from other areas
  - E.g. domain-specific terminologies, financial terminologies, ...
- *Rights Data Dictionary*:
  - Provides a general structure of terms ("*rights metadata*")
    - » <indecs> rdd: Verbs and Genealogies
  - Is open to integration of new terminologies
    - » Including "mix and match", e.g. several terminologies in one expression
  - Supports transformations between schemes
    - » By providing semantic relations between different schemes
- Similar to ontology languages, e.g. in the context of Semantic Web
- The "<indecs>" approach was originally developed for e-Commerce, and is the current baseline for the MPEG-21 RDD (see www.indecs.org)

Information and Content Exchange (ICE)

- Standard for *content syndication*
  - Exchange between businesses to re-bundle content (B2B processes)
  - Examples of syndication:
    - » Newspaper networks
    - » Marketing of movies to TV/Video (e.g. Buena Vista for Disney)
- Other examples of B2B content transactions:
  - Publishers licensing illustrations, tables, equations from other publishers
  - Regular content exchange among Web site providers, e.g. travel site getting restaurant reviews from another source
- ICE Standard (www.icestandard.org)
  - Supervised by IDEAlliance
  - Protocol expressed as XML vocabulary
  - Syndicators offer content to subscribers

Example of ICE-Based Syndication



Features of ICE

- Syndicators can...
  - Put up catalogues of content packages
  - Negotiate with subscribers
  - *Push* updated content packages to subscribers
  - Inform subscribers about news
- Subscribers can...
  - Browse syndicators' catalogues
  - Pull content packages
- ICE transfers include rules about digital rights
  - "ip-status" attribute for offers (license, public domain, free-with-ack etc.)
  - "rights-holder" attribute
  - Payment and reporting business terms

2 Digital Rights Management

Literature:

Bill Rosenblatt, Bill Trippe, Stephen Mooney: Digital Rights Management – Business and Technology, M&T Books 2002

Gerald Fränkl, Philipp Karpf: Digital Rights Management Systeme – Einführung, Technologien, Recht, Ökonomie und Marktanalyse, pg-Verlag 2004

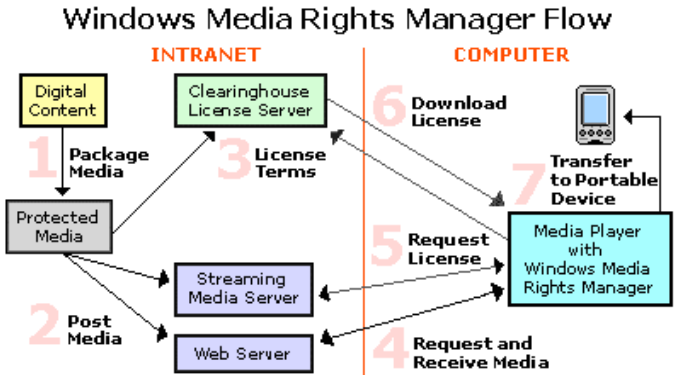
Pioneers of DRM

- InterTrust
  - "Electronic Publishing Resources" (1990-1997) did research in DRM base technology and filed many important patents
  - 1997: Name change to "InterTrust", marketing an end-to-end DRM-based publishing solution
  - 1999-2001: DRM products, many partnerships
  - 2004: $440 million deal with Microsoft on patent rights
- IBM infoMarket
  - 1994–1997 product targeted at an electronic marketplace which facilitates communication among independent sellers and buyers
  - Bases on original "superdistribution" idea
    - » "Cryptolopes" (Jeff Crigler) enabling distributed components to securely meter their usage and to initiate billing
    - » "Plug-N-Publish" toolkit for publishers (1995)
  - 1997 abandoned by IBM

Wave Systems

- www.wave.com
- www.wavexpress.com

Microsoft Windows DRM



- DRM built into recent versions of Windows Media Player

Apple FairPlay

- Apple's iTunes Music Store sells digital music in DRM-protected (encrypted) form
  - ".m4p" files: Protected MPEG-4 AAC files
  - MPEG-4 standard provides for "hooks" to be used by DRM
  - Apple encryption is proprietary ("AES CBC")
    - » Has been cracked already ("FairTunes")
- Relatively loose rights regulations:
  - Files may be used on up to 5 devices authorized to buying user
  - Unlimited burning of (unprotected) CDs
  - No restrictions to music ripped from CD
- Principles:
  - Identification of computer, obtained by hashing various local data
  - Central server checks authorization based on computer ID and sends decryption key which is stored locally in encrypted form dependent on computer ID

Beyond DRM: Alternative Proposals

- Electronic Frontier Foundation (EFF): www.eff.org
- John Perry Barlow (former lyricist for the *Grateful Dead*): The economy of ideas, *Wired* Magazine, Issue 2.03, March 1994

  www.wired.com/wired/archive/2.03/economy.ideas.html
  - Information wants to be free
  - Economy of information is different to economy of tangible goods:
    - » Value is in *familiarity* and *timeliness*, not scarcity
    - » Economy of relationship (real-time performance, services)
- Voluntary Collective Licensing
  - Flat rate for media sharing over the Internet (e.g. 5 €/month)
  - Paying the flat rate makes unlimited file sharing legal
  - Money is divided according to usage statistics and distributed back to artists (similar to ASCAP/BMI/GEMA system for radio broadcasts)

  http://www.eff.org/share/collective_lic_wp.php
- Music industry apparently moving towards less strict DRM systems
- Basic idea: ***Ethical*** principles, no brute-force technology approach