CS 155 Spring 2006

Digital Rights Management

John Mitchell

Next Tuesday

Paul Kocher
President and Chief Scientist
Cryptography Research, Inc.

2

Basic Problem

- Joey writes and records a song
  - Song distributed on some sort of media
  - Joey (and music company) want to *sell* recordings
  - But digital info is easy to copy, on most media
- What can Joey (and Music Inc.) try to do?
  - Look for copies?
  - Mark recording to make it easier to find copies?
  - Restrict media so only certain devices can play it?

All of these approaches have problems; no perfect solution (yet?)

3

Outline

- Examine or modify content
  - Content hashing and copyright crawling
  - Watermarking
  - Fingerprinting
- Regulate use through special content players
  - Apply complex policies, need tamper-proof platform
  - Some examples
    - MediaMax CD3: restrict access on software players
    - DVDs: CSS encryption and hardware/software players
    - Windows Media Rights Management
    - Office Information Rights Management

4

Content hashing

- Suppose we had a "content-aware" hash function:
  H: {music} → {short strings}
  satisfying:
  - 1. If M1 and M2 are two music clips (e.g. MP3 files) that play the "same" song then H(M1) = H(M2)
  - 2. Given a clip M a pirate cannot create an "acceptable" clip M' such that H(M) ≠ H(M')
- Is this realistic?
  - Hash function must resist all signal processing tricks
  - Do not know such hash functions exist
    - some claim to have them

5

Copyright Crawler

- Web crawler looks for copyright violations
  - Use list of hashes of all copyrighted content
  - Scans all web sites, Kazaa network, Napster, etc.
  - For every music file found, compute hash and compare
  - If match is found, call the lawyers
- Problems:
  - Hash functions unlikely to exist for music
  - Does not protect against anonymous postings: publius
  - Very high workload

6

Examples

- DigiMarc MarcSpider
  - Crawls web looking for pirated images
  - May use watermarking? (next topic)
- MOSS (Measure Of Software Similarity)
  - Detect plagiarism in programming assignments, web pages
  - http://www.cs.berkeley.edu/~aiken/moss.html
- SCAM: N. Shivakumar, Stanford.
  - Crawls web looking for academic plagiarism
  - Several success stories:
    http://www-db.stanford.edu/~shiva/SCAM/scamInfo.html

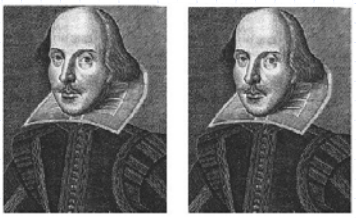
7

Improvement: watermarking

- Embed hidden watermark at the recording studio
  - Embed(M, I): outputs a watermarked version of music M with the information I embedded in it
  - Retrieve(M'): takes a watermarked music file M' and outputs the embedded watermark I
- Watermark requirements (not necessarily achievable):
  - Watermark must be inaudible
  - Watermark should be robust: Given M_1 = Embed(M,I), pirate cannot create an "acceptable" M_2 with Retrieve(M_2) ≠ I
    - To do this, watermark must resist all signal processing tricks - resampling, cropping, low-pass filtering, ...

8

Example Watermarked File



Second image has watermark inserted by DOS software "White Noise Storm"

9

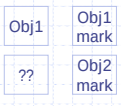
Watermark-based enforcement

- Copyright crawler uses "Retrieve" algorithm
- Benefits:
  - Copyright crawler does not need list of all copyrighted material
  - No need for content aware hash
    - Watermarking music "seems" to be an "easier" problem.
- But, some of the same problems as before
  - Does not defend against anonymous postings
  - High workload

10

Robust watermarks??

- Embed & Retrieve algs are usually kept secret
  - "Security by obscurity" – not a successful approach
- Do robust watermarking systems exist?
  - We don't know the answer
  - StirMark
    - Generic tool for removing image watermarks
    - Oblivious to watermarking scheme
  - SDMI challenge:
    - Broken: Felten, et al.



11

Fingerprinting

- Basic idea:
  - Embed a unique user ID into each sold copy
  - If user posts copy to web or Napster, embedded user ID identifies user
- Problem:
  - Need ability to create distinct and indistinguishable versions of object
  - Collusion: two users can compare their objects to find parts of the fingerprint

12

Watermarking Images (>200 papers)

- DigiMarc: embeds creator's serial number.
  - Add or subtract small random quantities from each pixel. Embedded signal kept secret.
- Signafy (NEC).
  - Add small modifications to random frequencies of entire Fourier Spectrum.
  - Embedded signal kept secret.
- Caronni: Embed geometric shapes in background.
- SigNum Tech. (SureSign).

13

Watermarking Music (>200 papers)

- Aris Tech (MusicCode):
  - Rate: 100 bits/sec of music
- Solana (E-DNA)
  - Used by LiquidAudio.

Merged to form Verance Used by SDMI

- Argent:
  - Embed full text information.
  - FrameBased: info. inserted at random areas of signal
  - Secret key determines random areas.

14

Some other issues

- Digital Millennium Copyright Act (DMCA)
  - Forbids circumvention of copy protection mechanisms, and circumvention tools and technologies
  - Some exceptions for security testing, law enforcement, research that aims to improve security
- Fair Use
  - Copyright law allows regulated use of copyrighted material in certain circumstances
    - Example: quote copyrighted material in a critical review

15

Disclaimer: I am not a lawyer. No statements in CS155 are legal advice.

"My Story" by Ed Felten

- Industry consortium (SDMI) considering four technologies for deployment in next-gen music and players.
- We (Princeton, Rice, Xerox researchers) study technologies, find that they don't work very well.
- We write a paper detailing our findings.
- Paper accepted for publication at conference.

3 Slides from: http://csrc.ncsl.nist.gov/ispab/2002-06/Felten-06-2002.pdf

16

"Our Paper"

- Music industry claims that our paper is a "technology" whose primary purpose is copyright circumvention
  - Similar claim for oral presentation
- Threatens to sue authors of paper, conference organizers, and employers
- Seeks control over contents of paper

17

"My Story (cont.)"

- Music industry (RIAA, SDMI, Verance) threatens lawsuit if we publish.
  - Conference organizers also threatened. We withdraw paper because of threats.
- We file lawsuit seeking right to publish
- After legal wrangling, paper is published
- We managed to publish, but:
  - Months of effort by researchers lost
  - Hundreds of lawyer-hours spent ($$$)
  - Member of our team loses his job
  - Eight-month delay in release of our results

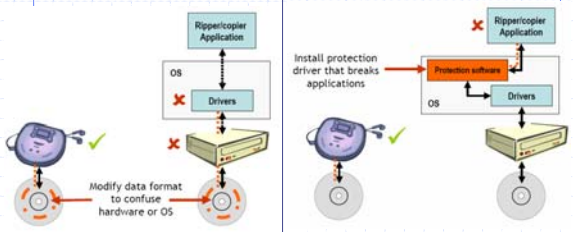
18

Outline

- Examine or modify content
  - Content hashing and copyright crawling
  - Watermarking
  - Fingerprinting
- Regulate use through special content players
  - Apply complex policies, need tamper-proof platform
  - Some examples
    - MediaMax CD3: restrict access for software players
    - DVDs: CSS encryption and hardware/software players
    - Windows Media Rights Management
    - Office Information Rights Management

19

Passive vs Active Protection



20

MediaMax CD3 (SunnComm)

- Goal
  - Restrict use of music CD on computer
- Method
  - CD contains autorun file that causes Windows to launch LaunchCD.exe, installs "SbcpHid" driver
  - Driver prevents copying of restricted CDs
- Failures
  - LaunchCD.exe will not run on Linux
  - On Windows: hold shift key while loading CD
- Digital Millennium Copyright Act (DMCA)
  - Forbids circumvention of copy protection mechanisms, and circumvention tools and technologies

http://www.cs.princeton.edu/~jhalderm/cd3/

21

Sony XCP

- CD contains copy protection software
- Copy protection software protected by rootkit
- Rootkit detected by RootkitRevealer

http://www.sysinternals.com/blog/2005/10/sony-rootkits-and-digital-rights.html

22

Content protection via encryption

- Basic idea:
  - Content distributor encrypts content before releasing it. Release: $C = E_K[\text{content}]$
  - Decryption key embedded in all players.
  - Player will only decrypt if policy is satisfied.
- Note: cannot prevent copying after decryption.
  - User can probe bus to sound card.
  - Unlike watermarking: watermark is embedded in content. Propagates in cleartext copies of content.
- Problem: what if one pirate uses reverse engineering to expose global key k ??

23

Example: CSS

- CSS: Content Scrambling System
  - Used to protect DVD movies.
- Each DVD player manufacturer i has key K_i, e.g. K_{sony}
  - Embed same key K_{sony} in all players from Sony.
  - Every DVD movie M is encrypted as follows:
    1. enc-content = $E_K[M]$; K – a random key.
    2. $E_{Ksony}[k]$, $E_{Kphilips}[K]$, ...
  - About 400 manufacturer keys

24

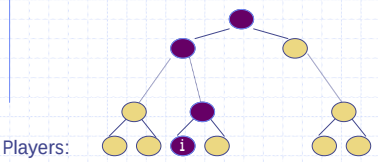
Problems with CSS

- DeCSS:
  - Extracted key from Xing software player
  - Could decrypt any DVD playable on the Xing player
  - MPAA revoked Xing key: disabled all Xing players!
- Bigger problem:
  - Encryption algorithm in CSS is based on LFSR's
  - Very fast: video rate decryption on weak DVD player
  - Very weak: given one manuf. Key, can get all keys

25

Better revocation technique

- Embed a distinct key in every player

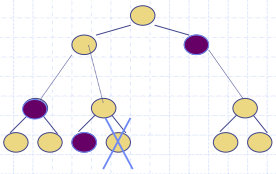


- Every node v has an associated key K_v.
- Every player corresponds to leaf node.
- Key for player i: all keys on path from root to leaf i.

26

Revocation

- Initially
  - Encrypt all content with key at root
  - Any player can decrypt content.
- When player i is revoked
  - Encrypt content-key so only players other than i can decrypt.



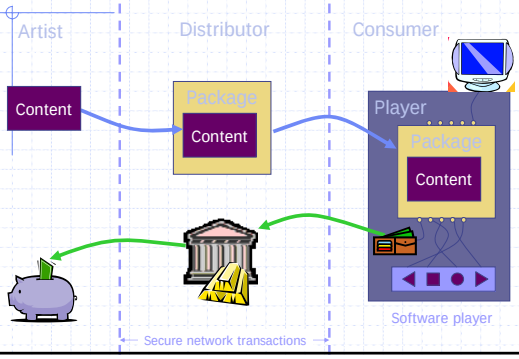
27

How to tell which player to revoke?

- When pirate publishes single key on Internet, MPAA knows which keys to revoke.
- What if pirate sells pirated players?
  - How can MPAA tell which keys embedded in player?
- Solution: Tracing systems can interact with player and determine how to revoke that player.
  - How? Take crypto class...

28

Digital Distribution Dream (Movies Books Music)



29

Digital rights management

- Distribute information in specific format
- Player that knows this format controls action
  - Control reading, playing, or copying content
  - Guarantee payment in proportion to use
    - Count number of times content is used
    - Transfer payment to distributor

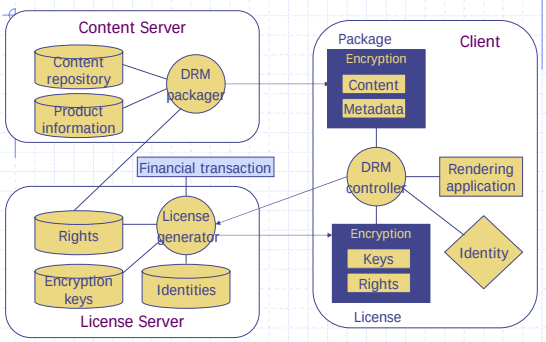
Problem: Computer files are easy to duplicate
Can software player on general-purpose computer achieve goals?

- No end run
  - Must be impossible to use content without player
  - Player must be tamper resistant

30

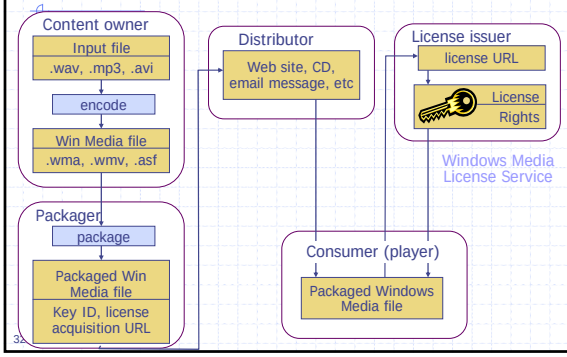
DRM Reference Architecture

Rosenblatt, et al.



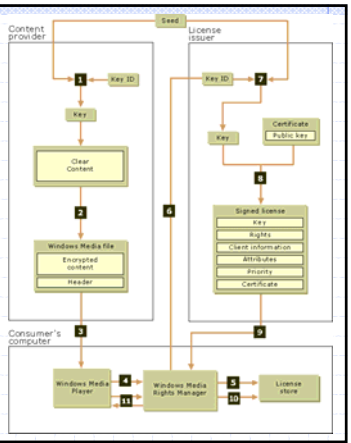
31

Windows Media Rights Manager



32

Windows Key and License Management



33

HDCP, Secure Audio Path

- High-bandwidth Digital Content Protection
  - HDCP is a specification developed by Intel Corporation to protect digital entertainment content across the DVI/HDMI interface

http://www.digital-cp.com/home

34

FreeMe – breaks Windows Media RM

- http://www....com/crypt/drm/freeme/README

  The software distributed with this README file removes content protection from any Windows Media Audio file (.wma file) that uses DRM version 2 (as implemented in Windows Media Player version 7). ...

- http://www...com/crypt/drm/freeme/Technical

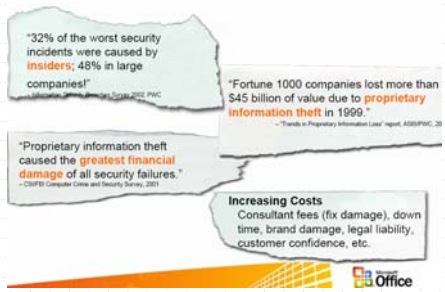
  This document describes version 2 of the Microsoft Digital Rights Management (MS-DRM), as applied to audio (.wma files). The sources for this material are varied ...

  The basic components of MS-DRM involve use of elliptic curve cryptography (ECC) for public key cryptography, DES for a block cipher, RC4 for a stream cipher, and SHA-1 for a hash function. There is also a block cipher which I haven't seen before, used in the MS-DRM system to build a MAC, or keyed hash function.

35

36

Microsoft Office Rights Management



37

www.microsoft.com/rms

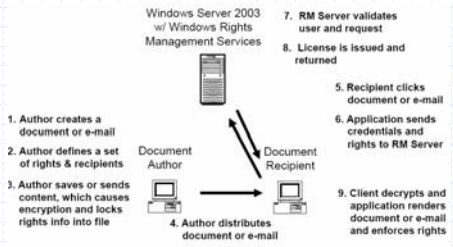
Information Rights Management Platform

- Server
  - Microsoft® Windows® Rights Management Services
  - Windows Server 2003
- Application
  - Information Rights Management (IRM)
  - Office 2003, IE Add On
- Protection goes with the file
  - File level, each gets its own protection
  - Persistent, goes wherever the file goes
- Controls Access and Usage
  - Encryption to help restrict access
  - Enforces usage policies in the application, e.g. disables print
  - Can expire content after it is no longer relevant

38

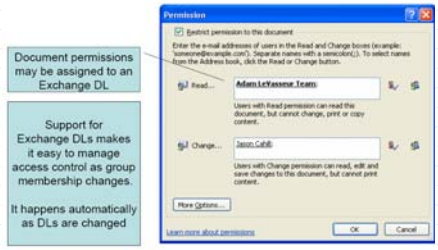
Slide graphics: Johann Kurz, Microsoft Schweiz GmbH, May '04 presentation

System schematic

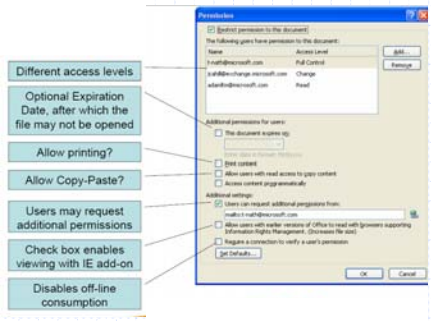


39

Authorizing user's UI

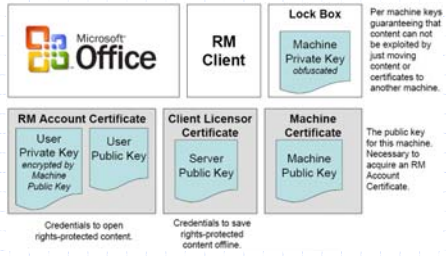


40



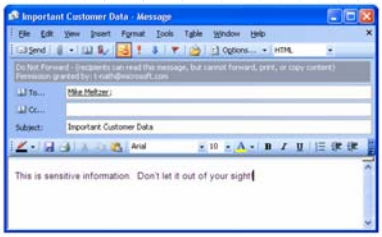
41

PC system components



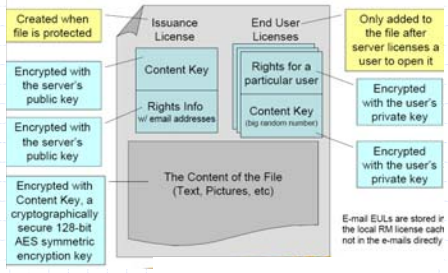
42

View of restricted email in Outlook



43

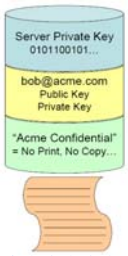
File contents



44

Server components

- Server's Private Key
- User Keys and addresses
  - User keys come from RMS when created
  - User addresses come from Active
  - Directory, which is required for RMS
- Permission Templates
- Logs
  - Logging occurs on creation and issuance of certificates and licenses and is IT controllable. Can be used as an audit trail.



45

XrML Summary

- Vocabulary
  - Principals: Alice, Bob
  - Resources: movie, picture, song
  - Rights: play, edit, print
  - Properties: manager, employee, trusted
- Licenses and grants
  - license ::= (grant, principal)
    - Principal p issues/says grant g
  - grant ::= $\forall x1 \ldots \forall xn$ (cond $\rightarrow$ conc)
    - If cond holds, then conc holds
  - conc ::= Pr(p) | Perm(p, r, s)
    - Pr(p) means principal p has property Pr
    - Perm(p, r, s) means p is permitted to exercise right r over resource s

46

Outline

- Examine or modify content
  - Content hashing and copyright crawling
  - Watermarking
  - Fingerprinting
- Regulate use through special content players
  - Apply complex policies, need tamper-proof platform
  - Some examples
    - MediaMax CD3: restrict access on software players
    - DVDs: CSS encryption and hardware/software players
    - Windows Media Rights Management
    - Office Information Rights Management

47

48