Digital Rights Management

and other protection mechanisms for author rights

Hans Georg Schaathun

Department of Computing
University of Surrey

26 June 2008

Myself

- Background in Coding Theory (University of Bergen)
- Current research interest
  - application of coding theory to digital watermarking
  - other areas of information security
- Lecturer at University of Surrey (40 min. South of London)
- CV available if you know of an open post near Sea and Mountains.

1. Introduction
   - Copyright Protection

2. Digital Rights Management
   - Typical DRM Solutions
   - Controversies
   - DRM-Security
   - Trusted Computing
   - Flexible solutions

3. Fingerprinting and Watermarking
   - Watermarking
   - Digital Fingerprinting
   - Deterring versus Prevention

4. Conclusions

The problem

- Creation is Expensive
- Copying is Cheap

Example

Logarithm Tables in ages past needed protection.

- Every figure computed manually (hoards of people)
- Reproduction (printing) relatively cheap
- ... leading to copyright piracy

- Today, computation is cheap
  - Logarithm Tables do not require protection

The digital problem

- What has changed in recent years?

The digital problem

- What has changed in recent years?
- Digital copies are perfect
  - Analogue copies (music cassettes, photocopies) are imperfect
- Amateur equipment is highly advanced
  - Perfect CD copies on your home PC

The digital problem

- What has changed in recent years?
- Digital copies are perfect
  - Analogue copies (music cassettes, photocopies) are imperfect
- Amateur equipment is highly advanced
  - Perfect CD copies on your home PC
- Cheaper and better quality for anyone
  - It always was possible...

Different Scenarios

- Large-scale and small-scale
  - Bob gave a copy to his best friend Polly
  - Oscar put the file on his web server
    - … downloaded by 1 345 823 arbitrary users
- Professional (profit-makers) versus careless amateurs
  - 242 643 rogue CD-s sold on a street markets in Calcutta
    - … criminals make millions …
  - Charlie(12) gave free copies to his 101 232 'friends' at facebook

Objective

Prevention versus Detection

- Prevent infringements
    - ... violations become impossible
- Detect and trace infringements
    - Prosecute violators – for penalties or for compensation
    - Deter potential violators
        - ... nobody is willing to risk a violation

Solutions

- Digital Rights Management (DRM)
  - Prevent copying
  - Limit copying and viewing
- Forensics and Investigation
  - Trace violators for prosecution
- Digital Fingerprinting – forensic aid

Possible Penalties

- Criminal justice: gaol and fines
- Civil law suit: compensation
- Revoke (disable) player
- Terminate subscription
- Penalty fees

Proprietary Solutions

- System requires a secret key in the player
    - Inaccessable for the user
    - Only trusted producers can make approved players
- Open standards would be impossible
    - ... no secret key
- Three main 'players'
    - Apple (i-tunes)
    - Microsoft
    - OMA – Open Mobile Alliance

The main players

- Apple and Microsoft are independent
  - Promote products of a single manufacturer
- Open Mobile Alliance (OMA)
  - Syndicate of 400 proprietary businesses
  - ... do not confuse it with an open standard
  - Licencing and approval from a syndicate
- How many partners can keep a secret?
  - The DVD-encryption was broken because one partner made a bug

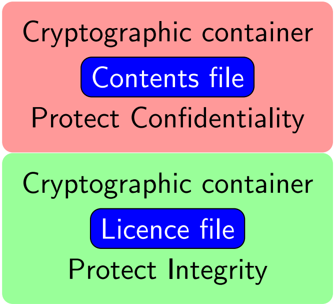
Function

- Prevent creation of working copies
- For example
  - Copies used only with original medium (computer games)
  - Copies play only on players belonging to licencee
  - Maximum of n copies can be made (e.g. *one* backup copy)
  - Viewing possible – printing impossible (e-libraries)

Traditional Fair Use

- Copies for personal use were traditionally legal
- Use copies with any player
  - traditional players are open technology (once patents expire)
  - once DRM contents is bought, you are locked to one brand
    - is your car player compatible with the one in your living room?
    - what if the manufacturer goes out of business?
- Do you treat all infringements the same?
  - A 10-year old schoolboy sharing files with a class mate
  - Organised crime selling bootleg copies *en masse*
- Traditional DRM cannot distinguish

The Data Object



Cryptographic container

Contents file

Protect Confidentiality

Cryptographic container

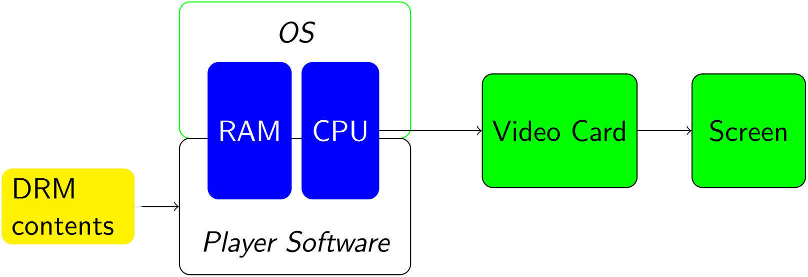
Licence file

Protect Integrity

- Contents and Licence may be separate
- Only trusted readers can decrypt contents
- Only trusted software update/create the licence

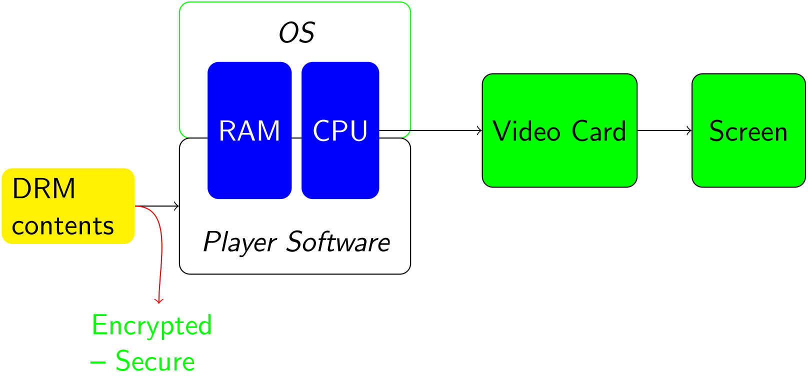
Software Player Architecture

Components



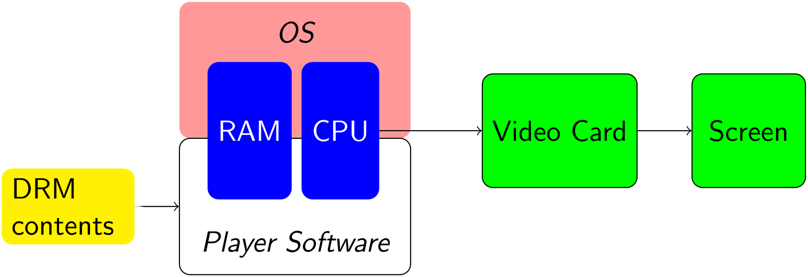
Software Player Architecture

The protection



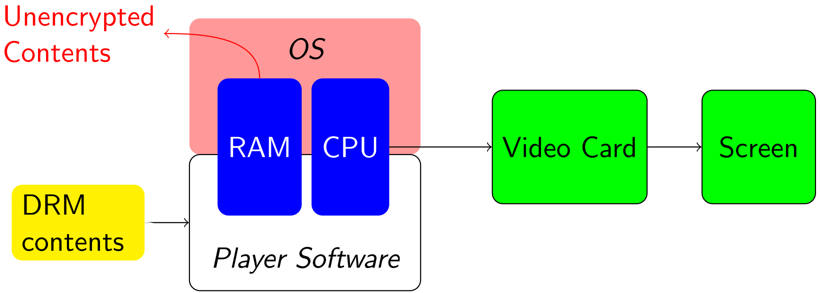
Software Player Architecture

The problem



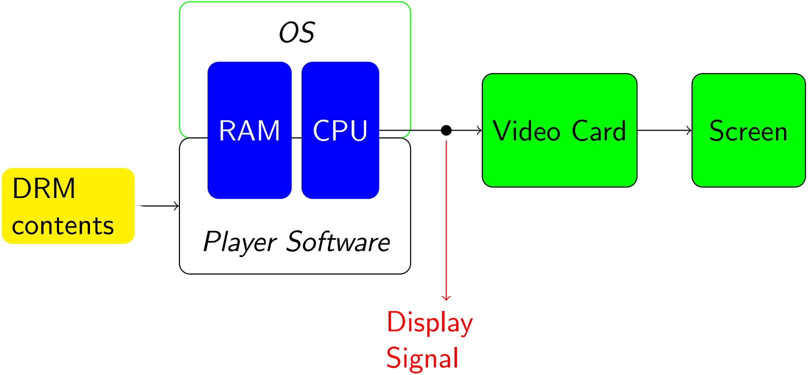
Software Player Architecture

The problem



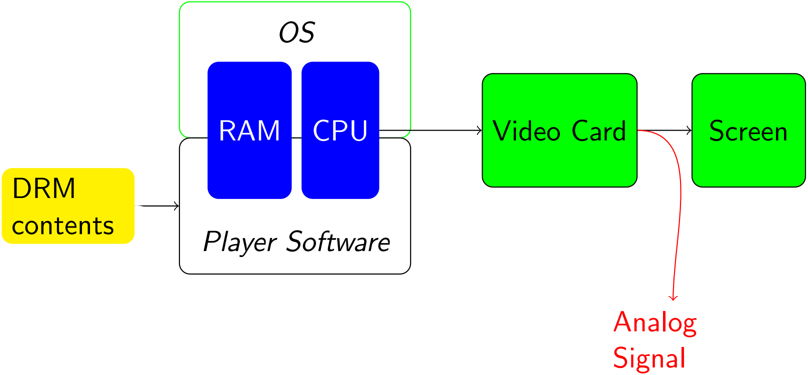
Software Player Architecture

The problem



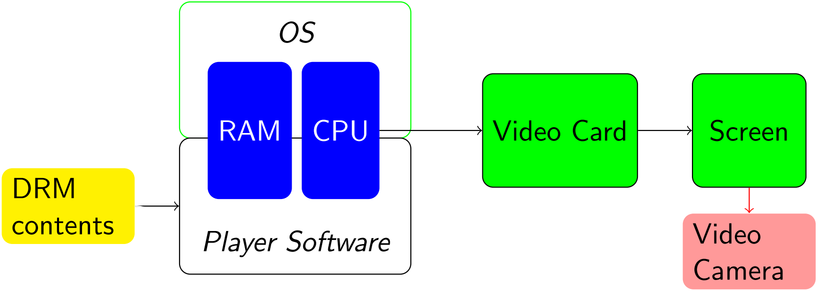
Software Player Architecture

The problem



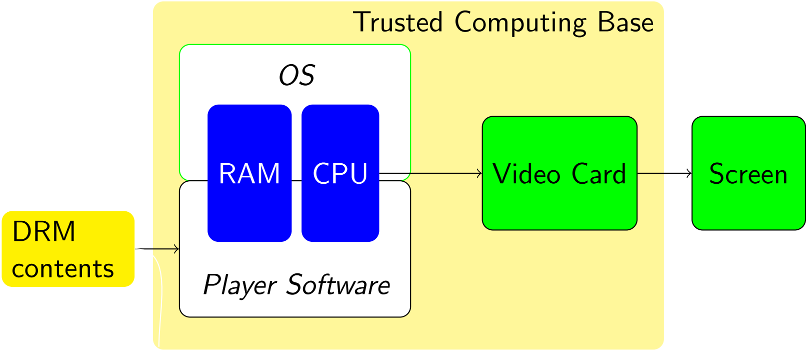
Software Player Architecture

The problem



Software Player Architecture

The solution



Analog leaks

- No protection against analog leaks
  - e.g. refilming with a separate camera
- Inferior quality
  - thus it might not be a problem
- Analog leaks possible at various stages
  1. Tapping the screen feed
  2. Re-filming
- At increasing level of quality loss
- How many do you have to protect?
  - and included in the trusted computing base?

Who owns the computer?

- Trusted computing is the principle that
  - software or data providers can trust the system

Who owns the computer?

- Trusted computing is the principle that
  - software or data providers can trust the system
- The *user* is not trusted

Who owns the computer?

- Trusted computing is the principle that
  - software or data providers can trust the system
- The *user* is not trusted
- Hence, software/data providers take partial control
  - User control is limited

Who owns the computer?

- Trusted computing is the principle that
  - software or data providers can trust the system
- The *user* is not trusted
- Hence, software/data providers take partial control
  - User control is limited
- So who is the rightful owner? Data provider or user?
- Can the user trust the data provider?

Sony XCP – as an example

- November 2005, Sony BMG recalled 2.1M CD-s [1]
  - they were too controversial
- Proprietary player required to play the CD on a PC
- Rootkit-type technology
  - modified the OS kernel
  - concealed itself
- Data supplier (partly) controls the customer PC

Does it work?

- Some solutions seem to keep providers happy
  - ... i-tunes have survived a long time
- Manufacturers seem not to believe in security
  - ... they require legal protection of the quasi-secure technology
- Security technology tends to be broken
  - ... organised criminals can generally get through
  - ... normaly people are prevented

Graceful Infringement Reactions

Katzenbeisser, Kursawe and Talstra (Philips) [2]

- Copying is not prevented
- Legal contents accompanied by a blacklist
- Player enforces penalties based on blacklist
- Pro: penalties can be tuned to severity of offence

The Player's Role

1. Playing
   - Any contents can be played
   - Contents played is watermarked
   - ... marked with the ID of the player
2. Enforcement
   - Whenever legal contents is aquired, a blacklist is supplied
   - Check for own ID in the blacklist
   - Enforce penalties based on violations listed

Contents Provider's Role

- Monitor the Internet (and other publication channels)
- Update blacklists
- Publish blacklists with authorised contents

Advantages

- Privacy
  - The monitor cannot identify the source
  - Only source player recognises its own identity
- Graceful reactions to different offences
  - Minor contents leaks deserve minor reactions
  - Large-scale distribution requires large-scale reactions

Digital Watermarking

Definition

Digital Watermarking refers to any technique to

- hide (modulate) a message in a host file
  - e.g. image, sound file
- preserving the use and value of the host file

How is it done?

- Redundancy of the host
    - small changes are imperceptible
- Say a 24-bit RGB pixmap image
    - change the *least significant bit* of each pixel/each component
    - Colour depth 24-bit → 21-bit
        - Who can tell the difference
    - Three bits per pixel to represent the hidden message

Robust Watermarking

Definition

Robust Watermarking refers to any watermarking technique where

- an attacker can neither destroy nor change the embedded watermark
- with non-negligible probability
- without also destroying the host file so beyond practical use

- Scenario-dependent definitions
  - 'Beyond practical use'
  - 'non-negligible probability'

Copyright applications

- Watermarks can contain
  - copyright notices – proof of ownership
  - ‘fingerprint’ – identifying the authorised user
    - ... to allow tracing of violators
  - DRM information – licencing information
    - Preventing contents and DRM information from being distributed separately

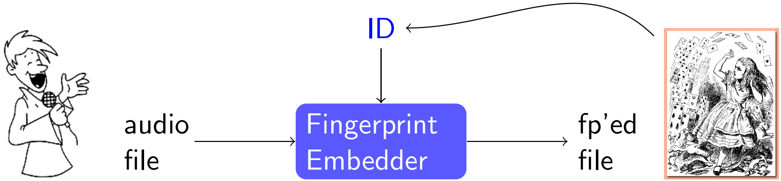
The threats

- A copyright violator attempts to disable the watermark
  - Remove all copyright-protection information
  - Change or add false proof of ownership
  - Change DRM information (e.g. rewind counters)
  - Change fingerprint (e.g. framing an innocent user)
- Robust Watermarking is appropriate

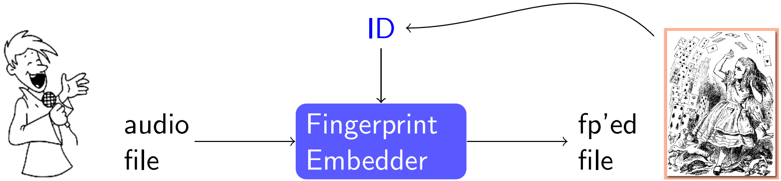
Is robust watermarking feasible?

- Well ... maybe
- Continuous improvements appear in the literature
- Especially for images
  - Robust against jpeg compression
  - Robust against printing and scanning
  - Robust against additive noise
  - Robust against rotation and cropping
- Hard to resist all attacks simultaneously
- Local geometric distortions is hard (Stirmark attack)
- Less research on Audio Watermarking (to date)

Digital Fingerprinting



Digital Fingerprinting



ID

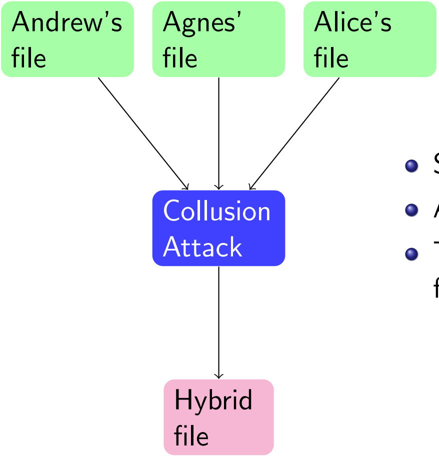
audio file

Fingerprint Embedder

fp'ed file

- Each copy sold contains the ID of the buyer
- If Charlie shows up with Alice's copy,
    - Alice can be prosecuted

Collusion Attacks



- Several copies ⇒ Extra information
- Averaging, cut-and-paste, etc.
- The hybrid carries no clean fingerprint

Collusion-Secure Codes

- Layered model
  - Coding layer: map user ID → codeword (fingerprint)
  - Embedding layer: hide fingerprint in copy
- Collusion-secure codes for the coding layer
  - Assume an abstract model
  - Robust against collusion attacks
- Embedding layer:
  - E.g. watermarking
  - Robust against other attacks (as other watermarking applications)
- Limitted by the state of the art in watermarking

Traitor Tracing in Broadcast Encryption

- Content is encrypted
  - subscribers have decoder boxes with a key
- Traitor Tracing protects the key
  - allows tracing of illegal decoder boxes

How it works

- Master key: matrix $K = [k_{i,j}]$ of keys
- User key: sequence $(k_{c_j,j} : j = 1 \dots n)$
    - one key per column of K
    - $(c_j : j = 1 \dots n)$ is a codeword from a collusion-secure code
- Session key: $\kappa = \kappa_1 + \kappa_2 + \dots + \kappa_n$
- Distribute an enabling block
    - $K_S = [E_{k_{i,j}}(\kappa_j)]_{i,j}$
    - κ can be calculated from K_S
        - if and only if one key per column of K is known
- Only known application where collusion-secure codes provably work.

The advantages of fingerprinting

- Fingerprinting is one component of the graceful reaction system of Katzenbeisser *et al*
- Technology applies only *after* the fact
- Irrelevant to innocent users
    - protects privacy and 'fair use'

The NDS Operational Security Unit

Len Withall [3]

- NDS distributes (among other things) Sky TV
- Operational Security Unit est. 1996
- Before ... decoder cards cracked within months
- The unit investigated piracy
    - tracing and prosecuting pirates
- Reputation that Sky cards are not worth cracking
- Sky P1 card remained secure for $4\frac{1}{2}$ year

Who needs protection?

- Big money at stake …
  - but how much?
  - and whose money?
- 85% of music recordings do not make money [RIAA]
  - proliferation of recordings means marketing
  - … increased revenue from live performance
- Loss estimates tend to assume that the alternative to an illegal copy is a legal copy paid for
  - Unlikely – it might mean fewer legal copies as well

The different solutions

- Prevention
- Forensics – detection and prosecution
- Fingerprinting – technological support for forensics
- Economic solutions
    - Maybe revenue could be ensured in different ways
    - ... research publications are now increasingly funded by the authors (or their sponsors)

Conclusion

- No perfect solution
  - Hard to prevent violations
  - and also protect fair use
- Security implies platform-dependence
- Fingerprinting allows fair use
  - ... but sufficient security is still an open question
- Forensic investigation has proved effective
- No authoritative study of socio-economic implications
  - ... and economic alternatives
- Maybe technology is the wrong way forward?

References

- M. Bishop and D. A. Frincke, “Who owns your computer?” *IEEE Security & Privacy*, pp. 61–63, March/April 2006.
- S. Katzenbeisser, K. Kursawe, and J. Talstra, “Graceful infringement reactions in drm systems,” in *DRM’06*, 2006.
- L. Withall, “Piracy hurts,” in *Crime and Security, The IET conference on*, Jun. 2006.
- W. Buhse and J. van der Meer, “The open mobile alliance digital rights management,” *IEEE Signal Processing Magazine*, pp. 140–143, Jan. 2007.
- P. Hunter, “Imagine there’s no drm ... i wonder if you can,” *Engineering and Technology*, pp. 36–40, Nov. 2006.