Weaknesses of DRM Systems

Hugo Jonker

hugo.jonker@uni.lu, h.l.jonker@tue.nl
SaToSS group, University of Luxembourg
FM group, Eindhoven University of Technology
On the one hand:

On the other:
On the one hand:
- creative minds...

On the other:
- curious society...
On the one hand:

- creative minds...
- desire to make a living.

On the other:

- curious society...
- benefits from access to creative ideas.
On the one hand:

- creative minds...
- desire to make a living.

On the other:

- curious society...
- benefits from access to creative ideas.

Copyright seeks to establish a balance between stimulation of innovation on the one hand, and dissemination of information on the other.
the law

Short, paraphrased summary:

✗ publishing of content without a right to do so.

✓ obtaining a copy for private use.

content - music, movies, books, ringtones, software games, etc.
“works of art”
Early digital content was “home-created”, and then “home-converted”.
**digital era**

- Early digital content was “home-created”, and then “home-converted”.

- Early copy control (e.g. cable tv, dvd):
  - static control
  - all-or-nothing access: access and content are bundled
Early digital content was “home-created”, and then “home-converted”.

Early copy control (e.g. cable tv, dvd):
- static control
- all-or-nothing access: access and content are bundled

Current situation:
- content is being exchanged on an enormous scale
- existing copy-protection measures are insufficient
Early digital content was “home-created”, and then “home-converted”.

Early copy control (e.g. cable tv, dvd):
- static control
- all-or-nothing access: access and content are bundled

Current situation:
- content is being exchanged on an enormous scale
- existing copy-protection measures are insufficient

Envisioned possibilities:
- digitised content that always stays copy protected
- tailor-made access for tailor-made prices
- opening a huge potential market
DRM purpose

DRM encompasses

- a new content protection mechanism
DRM purpose

DRM encompasses

- a new content protection mechanism
- for digital distribution
DRM purpose

DRM encompasses

- a new content protection mechanism
- for digital distribution
- providing dynamic access control
  - not just copy protection
DRM purpose

DRM encompasses

- a new content protection mechanism
- for digital distribution
- providing dynamic access control
  - not just copy protection
- focusing on practical security.
  - in absence of perfect security
DRM purpose

DRM encompasses

- a new content protection mechanism
- for digital distribution
- providing dynamic access control
  - not just copy protection
- focusing on practical security.
  - in absence of perfect security

Popular view: “keeping my music from me”
description of DRM systems

- network oriented technique
  internet, cable tv, cell phones, CD / DVD
description of DRM systems

- network oriented technique
  internet, cable tv, cell phones, CD / DVD

- govern distribution and protective measures of content
description of DRM systems

- network oriented technique
  internet, cable tv, cell phones, CD / DVD

- govern distribution and protective measures of content

- access control using licenses
  - access only when complying with a valid license, issued by certified license issuer
  - license specifies the access rights and conditions
  - license is typically non-transferable (i.e. bound)
  - unlicensed access should be “impossible”
core processes

creator | licensor | user

content creation | binding | license creation | processor | renderer

Weaknesses of DRM systems - p. 7/23

NLUUG voorjaarsconferentie, 15 May 2008
client side is untrusted...
...but should be able to render the content.
client dilemma

- client side is untrusted...
- ...but should be able to render the content.

Hence: trusted component (TCB) at client side needed.
Background: copy control

DRM systems
- description
- core processes
- client dilemma

Weaknesses

- Trusting the client
- Keeping content safe
- Security of DRM

Examples:
- MS DRM
- Apple iTunes

Final remarks

NLUUG voorjaarsconferentie, 15 May 2008
Main weak spots:

- the “analogue hole”,
- the entire client-side,
- the digital content.
trusted computing base

- a component that provides a trusted platform on which computations are performed

- properties:
  - computations cannot be inspected
  - computations cannot be disturbed

- Traditionally implemented in hardware (e.g. smartcard)
Conceptually impossible, but practically feasible.

Requirements:

- **Code tamper resistance**
  - e.g. software guards.

- **Data tamper resistance (secure storage)**
  - e.g. secure database.

- **Key hiding**
  - Data obfuscation.

- **Prevent “Break one, break ’em all” (BOBA) code obfuscation**
  - (individualisation).
software guards

- guards inserted at random points in the source code
- guards monitor specific areas of code
- guarded areas may overlap, may include guard(s)
- weak point: resolution procedure
secure container

- contains encrypted content, metadata, and possibly access restrictions and access rights

- restricts content access to “OK” by TCB (i.e. keeps content secret)

- can be exchanged unlimited

- opened by a valid license
Background: copy control

DRM systems

Weaknesses

Trusting the client

Keeping content safe

- secure container

-security container

Security of DRM

example: MS DRM

example: Apple iTunes

Final remarks
Practical security for internet DRM:

- TCB in hard- or software
- secure container
- secure client-side
- prevent “BOBA”
- updatability
Practical security for internet DRM:

- TCB in hard- or software
- secure container
- secure client-side
- prevent “BOBA”
- updataibility

is this sufficient?
about MS DRM

- uses Windows Media Player
- Hence a large installed base
- Hence many potential customers
- Hence opportunity to act as a service provider
- ongoing development, often renewed
- seems aimed at “full drm”
attacks on MS DRM

- **FreeMe**: recovers the TCB key.
  Problems: insufficient key hiding, BOBA.
attacks on MS DRM

- **FreeMe**: recovers the TCB key.
  Problems: insufficient key hiding, BOBA.

- MS response: strengthen individualisation.
attacks on MS DRM

- FreeMe: recovers the TCB key.
  Problems: insufficient key hiding, BOBA.

- MS response: strengthen individualisation.

- UnF...: captures output from player → audio out.
  Problem: insufficient client-side security
attacks on MS DRM

- **FreeMe**: recovers the TCB key.
  Problems: insufficient key hiding, BOBA.

  - MS response: strengthen individualisation.

- **UnF...**: captures output from player → audio out.
  Problem: insufficient client-side security

  - MS response: secure audio path.
attacks on MS DRM

- *FreeMe*: recovers the TCB key.  
  Problems: insufficient key hiding, BOBA.

- MS response: strengthen individualisation.

- *UnF...*: captures output from player $\rightarrow$ audio out.  
  Problem: insufficient client-side security

- MS response: secure audio path.

- etc.
about iTunes

- widely popular
- uses QuickTime and/or iPod player
- very successful (5 mln downloads in the first 8 weeks)

- lightweight licensing:
  - burn to CD
  - play on several computers
  - unlimited copying to iPods
**QTFairUse**: grabs digital output from player
attacks

- **QTFairUse**: grabs digital output from player
- **PlayFair / Hymn**: recovers TCB key (no key hiding, BOBA)
- **QTFairUse**: grabs digital output from player
- **PlayFair / Hymn**: recovers TCB key (no key hiding, BOBA)
- etc.
## DRM vs fair use: 0 - 1
conclusions

- DRM vs fair use: 0 - 1
- DRM vs analogue hole: 0 - 2
conclusions

- DRM vs fair use: 0 - 1
- DRM vs analogue hole: 0 - 2
- DRM in use: 1 - 3
conclusions

- DRM vs fair use: 0 - 1
- DRM vs analogue hole: 0 - 2
- DRM in use: 1 - 3
- DRM for online music: 1 - 4
conclusions

- DRM vs fair use: 0 - 1
- DRM vs analogue hole: 0 - 2
- DRM in use: 1 - 3
- DRM for online music: 1 - 4

retire DRM?
future of DRM

- cell phones
- navigation (maps)
- video on demand
- electronic health care

i.e. not the way envisioned by corporations (online music, big sales), but there are niches for DRM.
Thank you for your attention.

Questions?