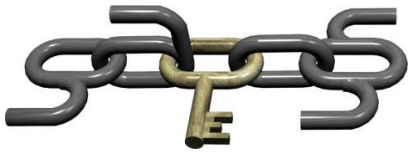


Weaknesses of DRM Systems

Hugo Jonker

hugo.jonker@uni.lu, h.l.jonker@tue.nl

SaToSS group, University of Luxembourg

FM group, Eindhoven University of Technology

precarious balance

On the one hand:

On the other:

precarious balance

On the one hand:

- creative minds...

On the other:

- curious society...

precarious balance

On the one hand:

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

On the other:

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

precarious balance

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:

x 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"

digital era

- 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

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

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
- 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 absense 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 absense 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

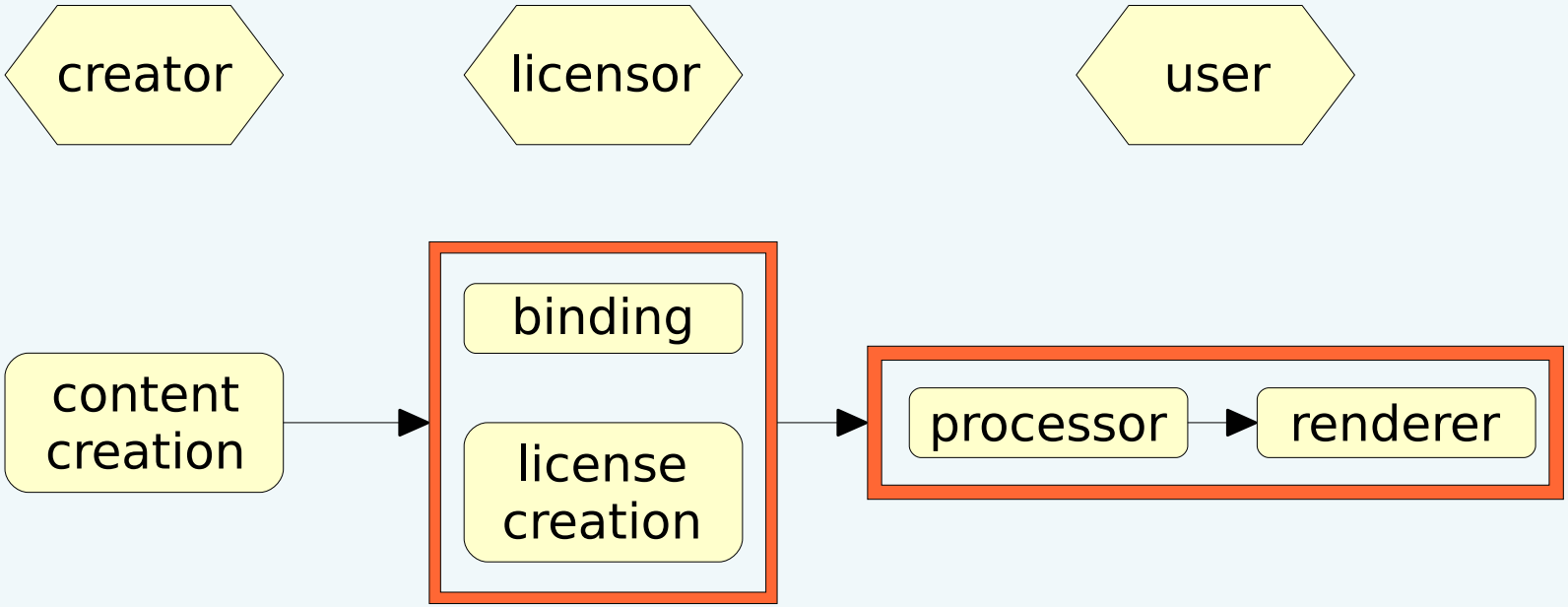
- network oriented technique

  internet, cable tv, cell phones, CD / DVD

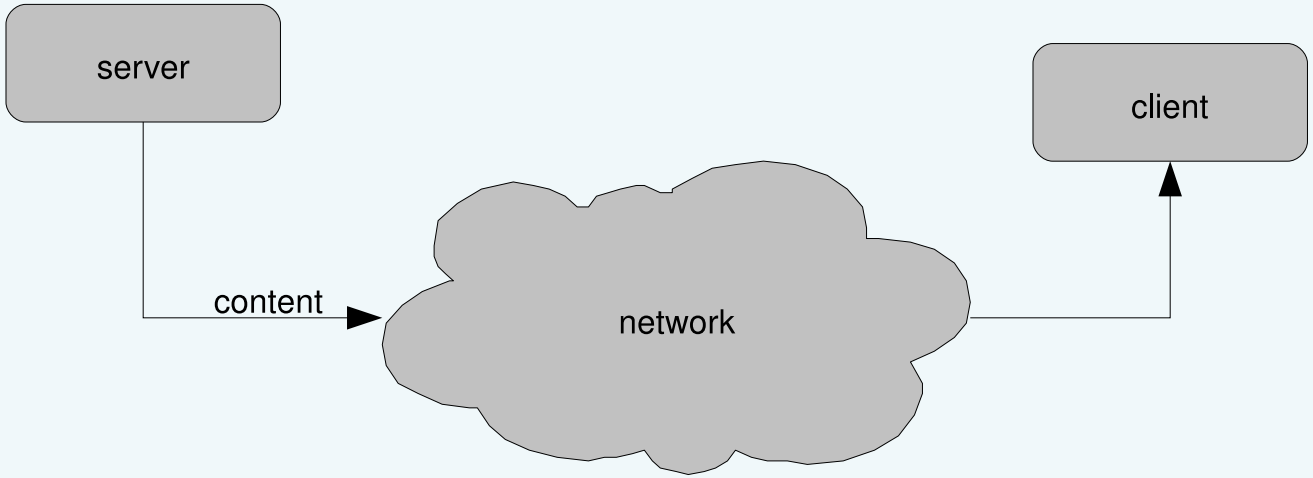
- govern distribution and protective measures of content

- 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

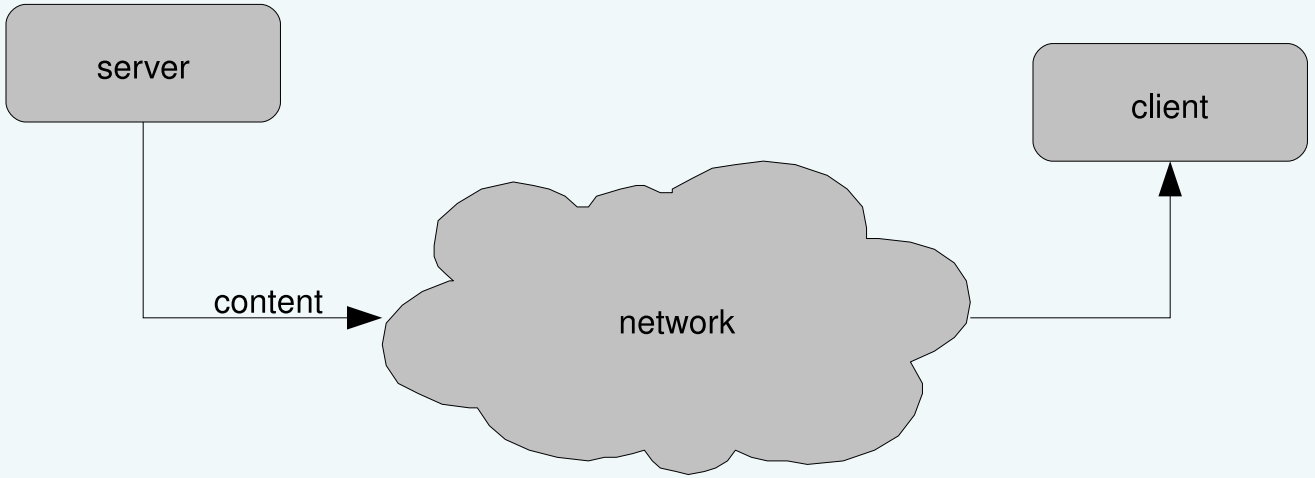


client dilemma



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

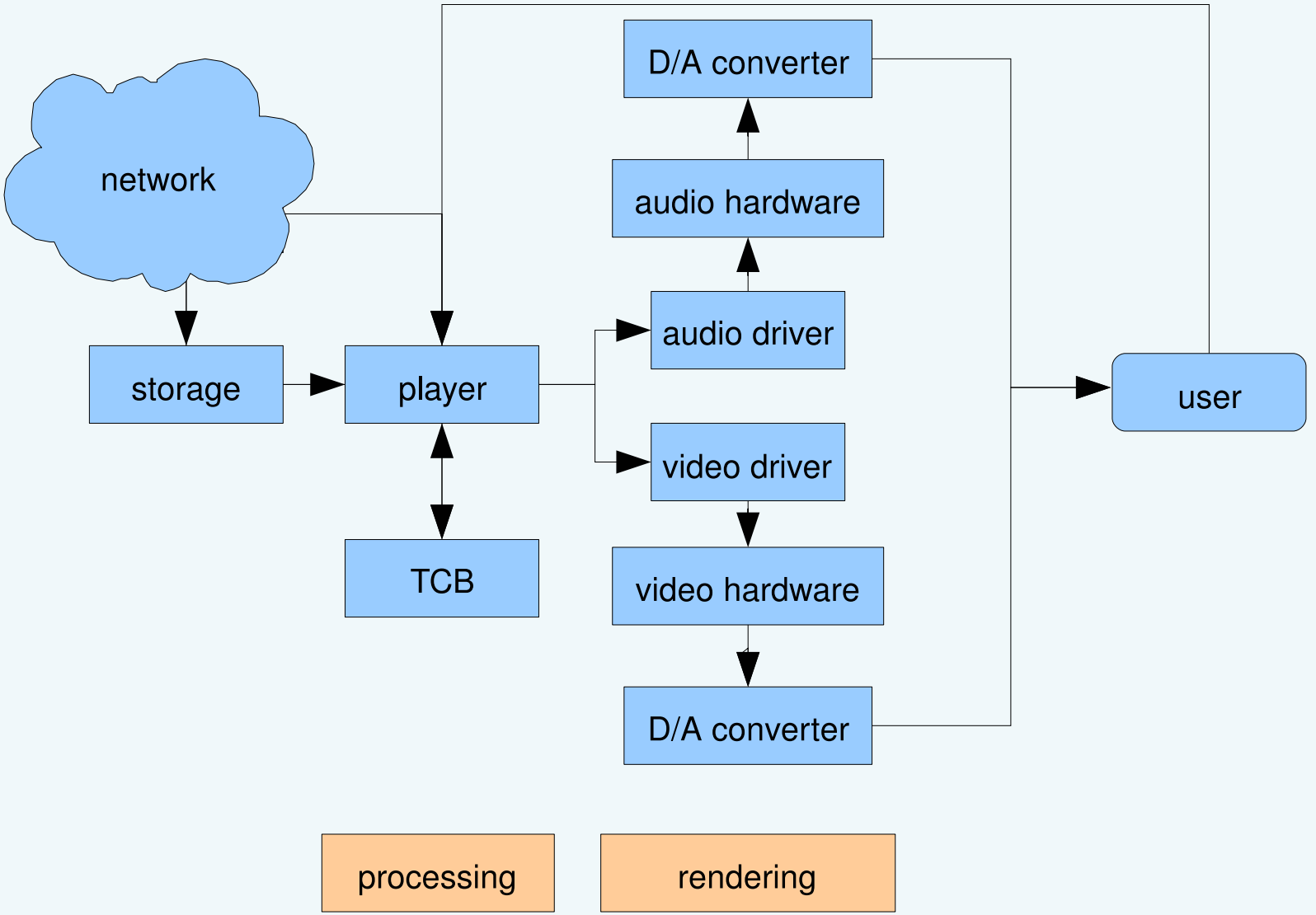
client dilemma



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

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

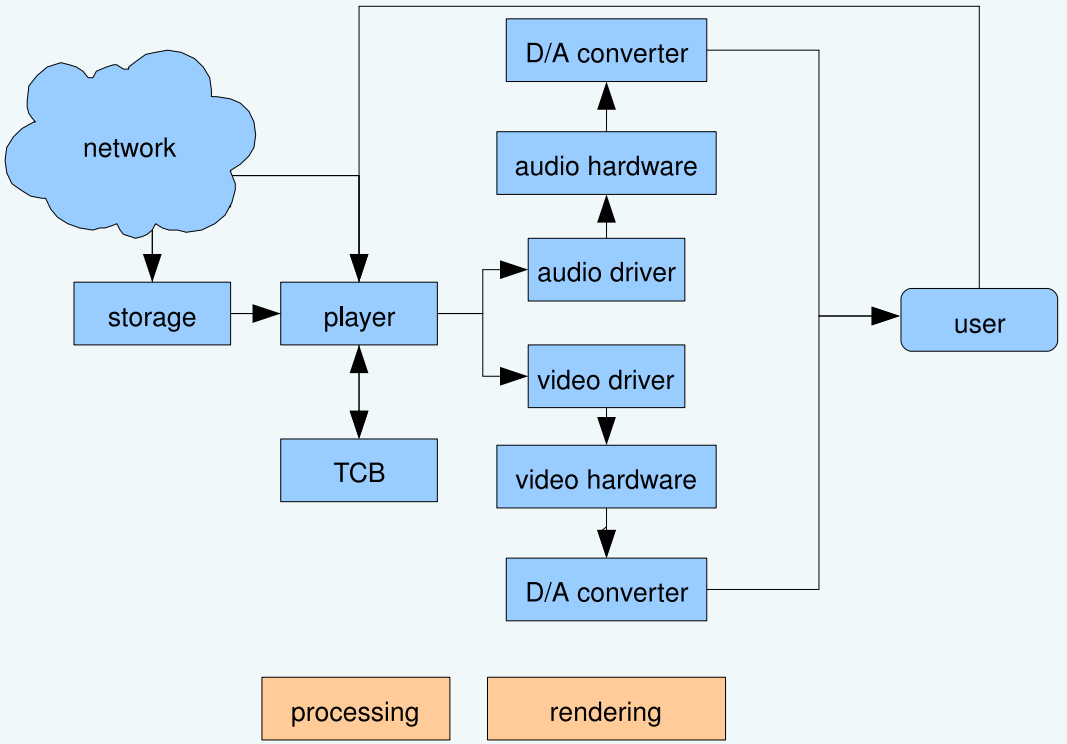
client-side



weak spots in DRM

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)

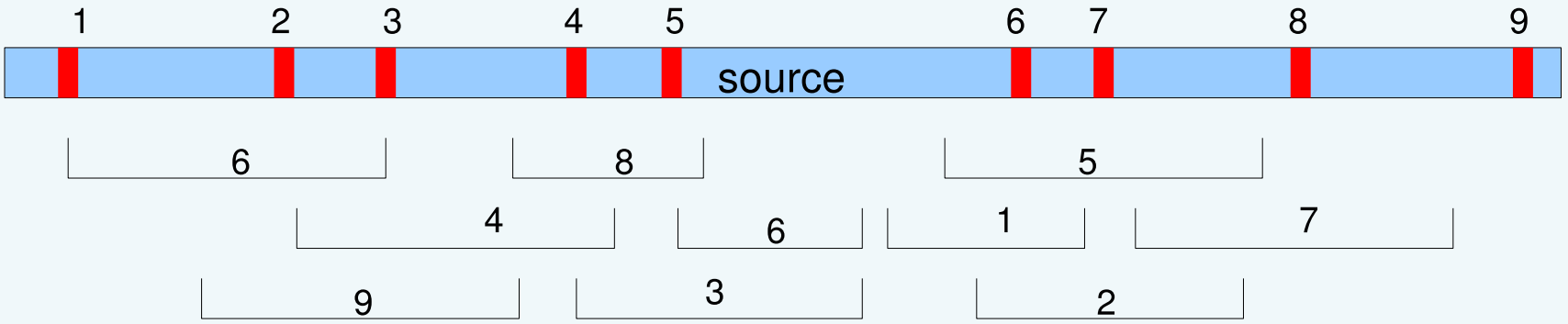
TCB in software

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



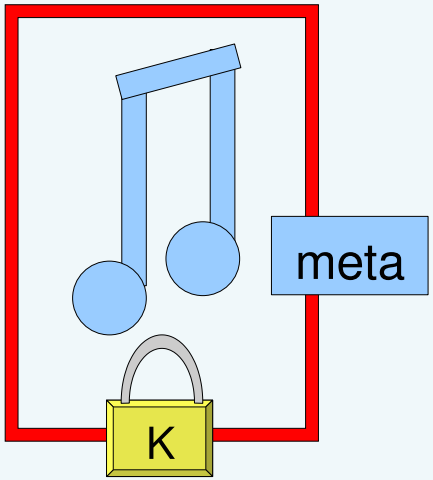
- guards inserted at random points in the source code
- guards monitor specific areas of code
- guarded areas may overlap, may include guard(s)

- weak point: resolution procedure

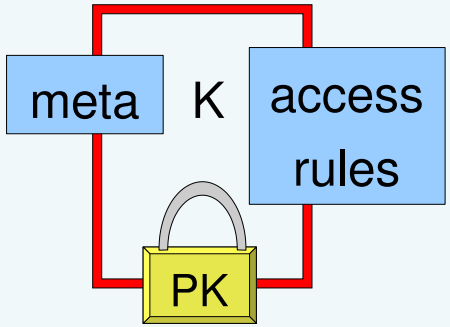
secure container

- 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

schematic



secure container



license

security measures

Practical security for internet DRM:

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

- updatability

security measures

Practical security for internet DRM:

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

- updatability

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 $\rightarrow$ 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 $\rightarrow$ 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.

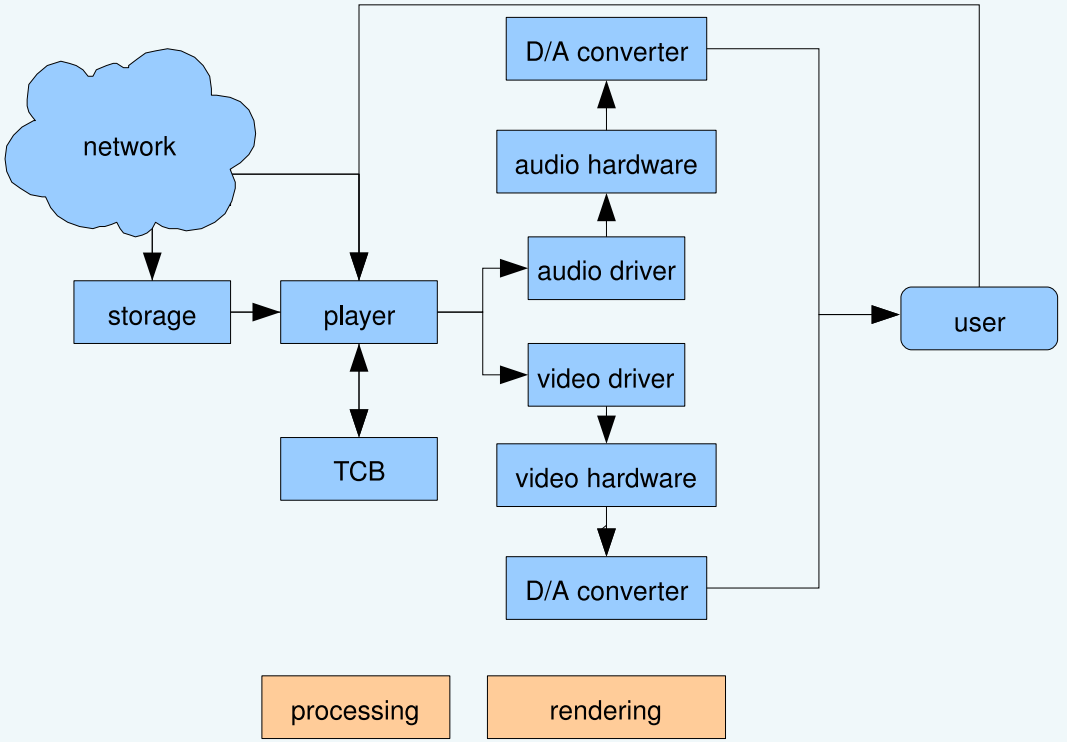
about iTunes

- 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

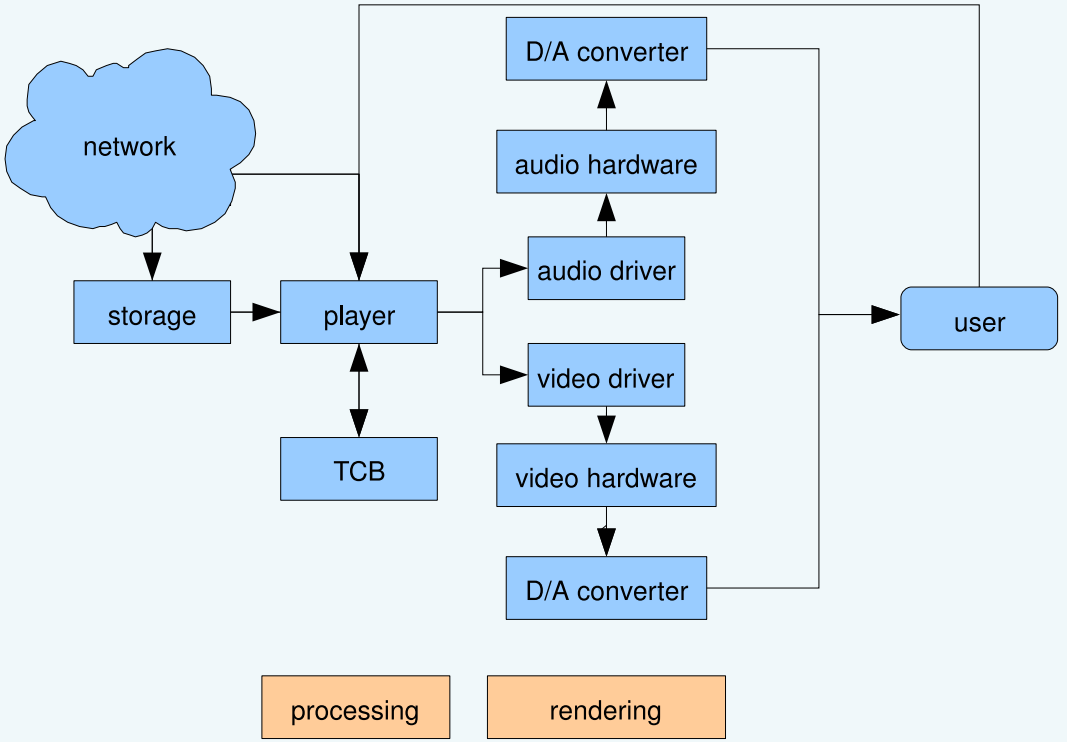
attacks

- *QTFairUse*: grabs digital output from player



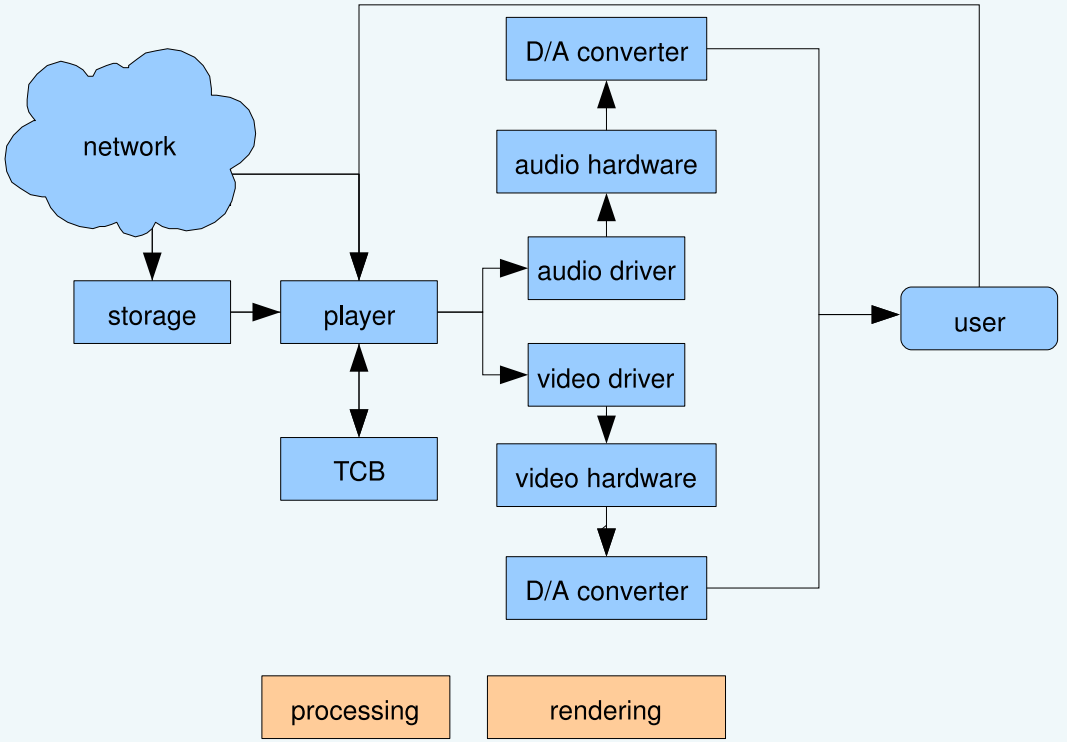
attacks

- *QTFairUse*: grabs digital output from player
- *PlayFair / Hymn*: recovers TCB key (no key hiding, BOBA)



attacks

- *QTFairUse*: grabs digital output from player
- *PlayFair / Hymn*: recovers TCB key (no key hiding, BOBA)
- etc.



conclusions

- 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.

final slide

Thank you for your attention.

Questions?