Security of
Digital Rights Management Systems

Hugo Jonker

SaToSS group, University of Luxembourg

FM group, Eindhoven University of Technology

collaborations: Sjouke Mauw (UL); Mohammad Dashti (CWI) and Srijith Nair (VU))

law

Copyright law ...

law

Copyright law ... seeks to establish a balance between ...

law

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

law

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

law

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

Specific use rights:

- private copies (fair use)
- resell right

digital era

- Early content protection systems (e.g. cable tv, dvd):
  - “binary” access control, no updates of access rights
  - content supplier also sells access rights

digital era

- Early content protection systems (e.g. cable tv, dvd):
  - “binary” access control, no updates of access rights
  - content supplier also sells access rights
- Currently:
  - digital content is being exchanged
  - existing copy-protection measures are insufficient

digital era

Copyright

- ● law
- ○ digital era
- ● “content”
- ● DRM purpose

DRM systems

Security

Security requirements

Nuovo DRM

Formal verification

Practical security

Conclusions

- Early content protection systems (e.g. cable tv, dvd):
  - “binary” access control, no updates of access rights
  - content supplier also sells access rights
- Currently:
  - digital content is being exchanged
  - existing copy-protection measures are insufficient
- Envisioned possibilities:
  - digitised content that remains copy protected indefinitely
  - tailor-made access for tailor-made prices

“content”

Copyright

- law
- digital era
- ○ “content”
- DRM purpose

DRM systems

Security

Security requirements

Nuovo DRM

Formal verification

Practical security

Conclusions

Examples of content:

“content”

Examples of content:

- music
- movies
- books
- ringtones
- software (games, applications)
- graphics (photo’s, logo’s, ...)

DRM purpose

- a new content protection mechanism...

DRM purpose

- a new content protection mechanism...
- for digital distribution...

DRM purpose

- a new content protection mechanism...
- for digital distribution...
- providing access control...
  - not just copy protection

DRM purpose

- a new content protection mechanism...
- for digital distribution...
- providing access control...
  - not just copy protection
- and have practical security.
  - in absense of perfect security (e.g. updatability)

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 bona fide license issuer
  - license specifies the access rights and conditions
  - license is typically non-transferable (i.e. bound)
  - unlicensed access should be impossible

network

two relevant types of network structures:

- client-server

  traditionally: content provider – customer
  DRM adds: license provider – customer

- peer-to-peer

  in DRM: client-to-client exchanges.

client-server

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

Hence, need for a trusted renderer (i.e. computing base) at client side.

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

Copyright

DRM systems

Security
- ● TCB
- ○ TCB in software
- ● secure container

Security requirements

Nuovo DRM

Formal verification

Practical security

Conclusions

conceptually impossible, but practically feasible.

requirements:

TCB in software

conceptually impossible, but practically feasible.

requirements:

- code tamper resistance

TCB in software

conceptually impossible, but practically feasible.

requirements:

- code tamper resistance
- data tamper resistance (secure storage)

TCB in software

Copyright

DRM systems

Security
- ● TCB
- ○ TCB in software
- ● secure container

Security requirements

Nuovo DRM

Formal verification

Practical security

Conclusions

conceptually impossible, but practically feasible.

requirements:

- code tamper resistance
- data tamper resistance (secure storage)
- key hiding

TCB in software

conceptually impossible, but practically feasible.

requirements:

- code tamper resistance
- data tamper resistance (secure storage)
- key hiding
- prevent “BORE”

TCB in software

conceptually impossible, but practically feasible.

requirements:

- code tamper resistance
- data tamper resistance (secure storage)
- key hiding
- prevent “BORE”

How to communicate with the TCB?

secure container

- encapsulation of content, metadata, and possibly access restrictions and access rights

secure container

- encapsulation of content, metadata, and possibly access restrictions and access rights

- enables secure communications with TCB (i.e. keeps content secret)

secure container

- encapsulation of content, metadata, and possibly access restrictions and access rights
- enables secure communications with TCB (i.e. keeps content secret)
- can be exchanged unlimited

secure container

- encapsulation of content, metadata, and possibly access restrictions and access rights
- enables secure communications with TCB (i.e. keeps content secret)
- can be exchanged unlimited
- opened by a valid license

establishing security requirements

High-level, conceptual analysis:

- establish stakeholders
- establish incentives
- derive core processes
- match incentives to processes

generic process model

Copyright

DRM systems

Security

Security requirements

● method

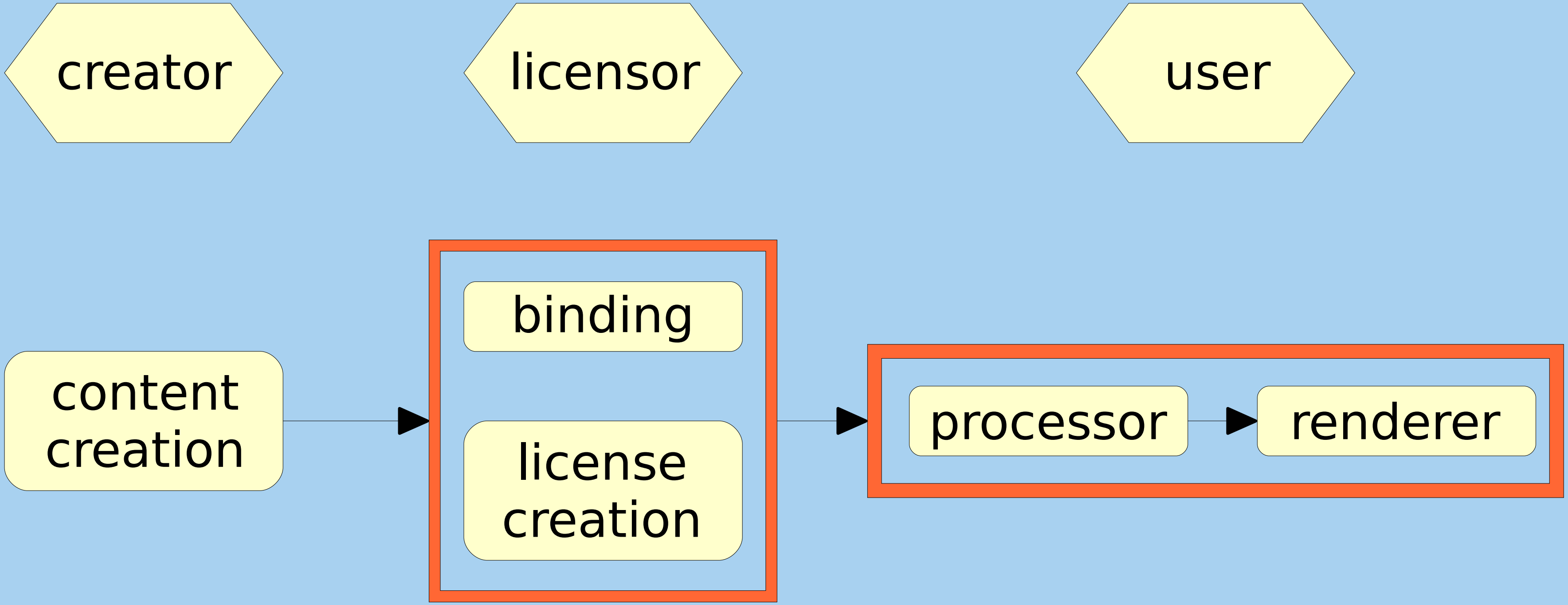
○ process model

Nuovo DRM

Formal verification

Practical security

Conclusions



objectives

- enable fair C2C exchanges ... (as NPGCT)
- ... whilst preserving DRM (unlike NPGCT)
- verify security of the scheme...
- *and* have a practical stance towards security

intruder

For formal verification, assume the standard Dolev-Yao intruder, except:

- trusted devices comply with specification...
- ...but may be turned off prematurely by their owner
- assume resilient channels to enable fairness

goals

- effectiveness
- secrecy
- resist content masquerading
- fairness of exchange

expressed in μ-calculus, e.g. (content masquerading):

goals

Copyright

DRM systems

Security

Security requirements

Nuovo DRM

Formal verification

● intruder

○ goals

● analysis

Practical security

Conclusions

- effectiveness
- secrecy
- resist content masquerading
- fairness of exchange

expressed in μ-calculus, e.g. (content masquerading):

$$\begin{aligned}
&\forall c \in \mathit{Content},\ r \in \mathit{Rights}.\\
&\qquad [(\neg \mathit{request}(d1, c, r, d2))^{*}.\mathit{update}(d1, c, r, d2)]\text{False} \ \wedge\\
&\qquad [(\neg \mathit{request}(d2, c, r, d1))^{*}.\mathit{update}(d2, c, r, d1)]\text{False} \ \wedge\\
&\qquad [(\neg \mathit{request}(d1, c, r, P))^{*}.\mathit{update}(d1, c, r, P)]\text{False} \ \wedge\\
&\qquad [(\neg \mathit{request}(d2, c, r, P))^{*}.\mathit{update}(d2, c, r, P)]\text{False}.
\end{aligned}$$

analysis

- Nuovo modelled in μCRL
- analysed scenario's:
  1. 2 devices, no intruder, synchronous communication (effectiveness)
  2. 2 devices, intruder, asynchronous communication (secrecy, content masquerading, fairness)
- result:

remarks:

analysis

- Nuovo modelled in μCRL
- analysed scenario's:
  1. 2 devices, no intruder, synchronous communication (effectiveness)
  2. 2 devices, intruder, asynchronous communication (secrecy, content masquerading, fairness)
- result: Nuovo meets goals!

remarks:

analysis

- Nuovo modelled in μCRL

- analysed scenario's:
  1. 2 devices, no intruder, synchronous communication (effectiveness)
  2. 2 devices, intruder, asynchronous communication (secrecy, content masquerading, fairness)

- result: Nuovo meets goals!

remarks:

- limited scenario
- several assumptions (e.g. trusted devices)

procedures

- resolving C2C disputes by the provider
- detection of compromised devices
- revocation of compromised devices

revocation of compromised devices

revocation list properties:

- per-device list size
- effectiveness

distribution schemes:

revocation of compromised devices

revocation list properties:

- per-device list size
- effectiveness

distribution schemes:

- *complete copy:* copy the entire RL
- *friends-check:* only contacted devices

revocation of compromised devices

Copyright

DRM systems

Security

Security requirements

Nuovo DRM

Formal verification

Practical security

● procedures

○ revocation

Conclusions

revocation list properties:

- per-device list size
- effectiveness

distribution schemes:

- *complete copy:* copy the entire RL
- *friends-check:* only contacted devices
- *propagated list:* friends-check; but forward all

revocation of compromised devices

revocation list properties:

- per-device list size
- effectiveness

distribution schemes:

- *complete copy:* copy the entire RL
- *friends-check:* only contacted devices
- *propagated list:* friends-check; but forward all
- *restricted propagation:* propagate; but only own list

Copyright

DRM systems

Security

Security requirements

Nuovo DRM

Formal verification

Practical security

● procedures

○ revocation

Conclusions

revocation of compromised devices

revocation list properties:

- per-device list size
- effectiveness

distribution schemes:

- *complete copy:* copy the entire RL
- *friends-check:* only contacted devices
- *propagated list:* friends-check; but forward all
- *restricted propagation:* propagate; but only own list

$$d1 \leftrightarrow P\colon\ \mathit{self}_{d1} := \mathit{friends}_{d1} \cap \mathit{drl}.$$

$$d1 \leftrightarrow d2\colon\ \mathit{rest}_{d1}, \mathit{friends}_{d1} := \mathit{rest}_{d1} \cup \mathit{self}_{d2}, \mathit{friends}_{d1} \cup \{d\}.$$

conclusions & future work

Conclusions:

Future work:

conclusions & future work

Conclusions:

- saw an overview of security of DRM systems

Future work:

conclusions & future work

Conclusions:

- saw an overview of security of DRM systems
- process model serves as basis for establishing security requirements

Future work:

conclusions & future work

Conclusions:

- saw an overview of security of DRM systems
- process model serves as basis for establishing security requirements
- C2C exchanges possible whilst preserving DRM

Future work:

conclusions & future work

Conclusions:

- saw an overview of security of DRM systems
- process model serves as basis for establishing security requirements
- C2C exchanges possible whilst preserving DRM
- a practical stance towards security remains important

Future work:

conclusions & future work

Conclusions:

- saw an overview of security of DRM systems
- process model serves as basis for establishing security requirements
- C2C exchanges possible whilst preserving DRM
- a practical stance towards security remains important

Future work:

- formalise accountability of provider, privacy concerns, payment

conclusions & future work

Conclusions:

- saw an overview of security of DRM systems
- process model serves as basis for establishing security requirements
- C2C exchanges possible whilst preserving DRM
- a practical stance towards security remains important

Future work:

- formalise accountability of provider, privacy concerns, payment
- investigate effectiveness of revocation list in more complex settings

final slide

Thank you for your attention

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