# Nuovo DRM Paradiso

## Towards a verified, fair DRM protocol

Hugo Jonker h.l.jonker@tue.nl

Srijith Krishnan Nair srijith@few.vu.nl

Mohammad Torabi Dashti dashti@cwi.nl

# Digital Rights Management

- Goal:
  - restrict access to *content* (movies, music, ...)
  - access granted only when complying with *license*

# Digital Rights Management

- Goal:
  - restrict access to *content* (movies, music, ...)
  - access granted only when complying with *license*
- Method:
  - enforce link by bundling license with encrypted content

# Digital Rights Management

- Goal:
  - restrict access to *content* (movies, music, ...)
  - access granted only when complying with *license*
- Method:
  - enforce link by bundling license with encrypted content
- Environment:
  - trusted devices
  - trusted content providers

# Digital Rights Management

- Goal:
  - restrict access to *content* (movies, music, ...)
  - access granted only when complying with *license*
- Method:
  - enforce link by bundling license with encrypted content
- Environment:
  - trusted devices
  - trusted content providers
- Intruder:
  - untrusted device owners
  - untrusted network

# Enabling C2C exchange

- bottleneck in provider-to-client exchanges: bandwidth

# Enabling C2C exchange

- bottleneck in provider-to-client exchanges: bandwidth
- solution: enable client-to-client exchanges...

# Enabling C2C exchange

- bottleneck in provider-to-client exchanges: bandwidth
- solution: enable client-to-client exchanges...
- ... whilst preserving DRM

# Enabling C2C exchange

- bottleneck in provider-to-client exchanges: bandwidth
- solution: enable client-to-client exchanges...
- ... whilst preserving DRM

Adapt intruder model:

# Enabling C2C exchange

- bottleneck in provider-to-client exchanges: bandwidth
- solution: enable client-to-client exchanges...
- ... whilst preserving DRM

Adapt intruder model:

- complete, lasting protection unrealistic...

# Enabling C2C exchange

- bottleneck in provider-to-client exchanges: bandwidth
- solution: enable client-to-client exchanges...
- ... whilst preserving DRM

Adapt intruder model:

- complete, lasting protection unrealistic...
- thus: migitation procedures:
  - detection
  - revocation list

# Weaknesses

1. P2C: no link between content request and received rights
   attack: insert rights

# Weaknesses

1. P2C: no link between content request and received rights
   attack: insert rights

2. C2C: No link between delivery of content and payment
   attack: abort before paying

# Intuition

*“Either both parties terminate successfully, or none does”*

- Not possible without TTP ⇒ overhead!

Optimistic fair exchange:

- only use TTP if fairness violated otherwise
- protocols:
  - optimistic exchange (no TTP)
  - finish succesfully (using TTP)
  - abort all commitments (using TTP)

# Fair exchange in DRM

- DRM assumption: trusted devices, untrusted device *owners*
  ⇒ devices may be halted, but otherwise comply
- exchange in DRM: content for money
  - abort before either exchanged
    ⇒ no problem
  - abort after both exchanged
    ⇒ succesful termination
  - abort after one, before other
    ⇒ not fair...

# Achieving FE in DRM

How to introduce fair exchange?
(Tip: first address the question: who can be TTP?)

Hints:

# Achieving FE in DRM

How to introduce fair exchange?
(Tip: first address the question: who can be TTP?)

Hints:

- will anyone give you money if you didn’t receive it?

# Achieving FE in DRM

How to introduce fair exchange?
(Tip: first address the question: who can be TTP?)

Hints:

- will anyone give you money if you didn’t receive it?
- can anyone provide content if you didn’t receive it?

# Achieving FE in DRM

How to introduce fair exchange?
(Tip: first address the question: who can be TTP?)

Hints:

- ■ will anyone give you money if you didn’t receive it?
- ■ can anyone provide content if you didn’t receive it?

Solution:

# Achieving FE in DRM

How to introduce fair exchange?
(Tip: first address the question: who can be TTP?)

Hints:

- will anyone give you money if you didn’t receive it?
- can anyone provide content if you didn’t receive it?

Solution:

- provider = TTP

# Achieving FE in DRM

How to introduce fair exchange?
(Tip: first address the question: who can be TTP?)

Hints:

- will anyone give you money if you didn't receive it?
- can anyone provide content if you didn't receive it?

Solution:

- provider = TTP
- first exchange money, then content

# Achieving FE in DRM

How to introduce fair exchange?
(Tip: first address the question: who can be TTP?)

Hints:

- will anyone give you money if you didn't receive it?
- can anyone provide content if you didn't receive it?

Solution:

- provider = TTP
- first exchange money, then content
- no abort protocol necessary!

# Achieving FE in DRM

How to introduce fair exchange?
(Tip: first address the question: who can be TTP?)

Hints:

- will anyone give you money if you didn’t receive it?
- can anyone provide content if you didn’t receive it?

Solution:

- provider = TTP
- first exchange money, then content
- no abort protocol necessary!
- relies on compliance of devices

# Design

Motivation:

Goals of Nuovo:

# Design

Motivation:

- address weaknesses
- increase assurance of security

Goals of Nuovo:

# Design

Motivation:

- address weaknesses
- increase assurance of security

Goals of Nuovo:

- effectiveness
- secrecy
- resist content masquerading
- fairness

# P2C protocol

## Provider — client exchange

$P$: provider; $C$: client; $M$: content; $R$: rights

$$\begin{array}{lrl}
1. & owner(C) \rightarrow C: & P,\ h(M),\ R \\
2. & C \rightarrow P: & C,\ n_C \\
3. & P \rightarrow C: & \{n_P,\ n_C,\ C\}_{sk(P)} \\
4. & C \rightarrow P: & \{n_C,\ n_P,\ h(M),\ R,\ P\}_{sk(C)} \\
5. & P \rightarrow C: & \{M\}_K,\ \{K\}_{pk(C)},\ \{R,\ n_C\}_{SK(P)}
\end{array}$$

- concrete protocol
- first weakness addressed (validity of $R$)

# C2C protocols

Client — client optimistic exchange:

*similar to P2C for clients* $C, D$

Client — client, recovery:

$$\begin{array}{lrl}
5^r. & D: & resolves(D) \\
6^r. & D \rightarrow P: & D,\ n'_D \\
7^r. & P \rightarrow D: & \{n_P,\ n'_D,\ D\}_{sk(P)} \\
8^r. & D \rightarrow P: & \{n'_D,\ n_P,\ \langle n_D,\ n_C,\ h(M),\ R',\ C\rangle,\ P\}_{sk(D)} \\
9^r. & P \rightarrow D: & \{M\}_K,\ \{K\}_{pk(D)},\ \{R',\ n'_D\}_{SK(P)}
\end{array}$$

# Formal analysis

Modelling in $\mu$CRL:

- Nuovo DRM
- communication model
- intruder model – Dolev-Yao, with restrictions

Analysed scenario's:

1. no intruder, synchronous communication (effectiveness)
2. intruder, asynchronous communication (secrecy, masquerading, fairness)

# Analysis results

Introduction

NPGCT Scheme

Fair Exchange

Nuovo DRM

Assessment
● Formal analysis
○ Analysis results

Conclusions

Modelled scenario’s checked with CADP:

- effectiveness
- secrecy
- resisting content masquerading
- fairness

# Analysis results

Modelled scenario's checked with CADP:

- √ effectiveness
- – secrecy
- – resisting content masquerading
- – fairness

# Analysis results

Modelled scenario's checked with CADP:

- √ effectiveness
- √ secrecy
- – resisting content masquerading
- – fairness

# Analysis results

Modelled scenario's checked with CADP:

- $\surd$ effectiveness
- $\surd$ secrecy
- $\surd$ resisting content masquerading
- – fairness

# Analysis results

Modelled scenario’s checked with CADP:

- ✓ effectiveness
- ✓ secrecy
- ✓ resisting content masquerading
- ✓ fairness

# Concluding

- Identified weaknesses in NPGCT
- Designed improvement: Nuovo DRM Paradiso
- Formally verified design goals
- Provide a reworked revocation method

# Concluding

- Identified weaknesses in NPGCT
- Designed improvement: Nuovo DRM Paradiso
- Formally verified design goals
- Provide a reworked revocation method

Thank you for your attention!