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
Goal:
- restrict access to digital *contents*
- access granted only when complying with *license*
Goal:
- restrict access to digital *contents*
- access granted only when complying with *license*

Method:
enforce link by bundling license with content
Digital Rights Management

- **Goal:**
  - restrict access to digital *contents*
  - access granted only when complying with *license*

- **Method:**
  enforce link by bundling license with content

- **Environment:**
  - trusted devices (well...)
  - trusted content providers
Digital Rights Management

- Goal:
  - restrict access to digital *contents*
  - access granted only when complying with *license*

- Method:
  enforce link by bundling license with content

- Environment:
  - trusted devices (well...)
  - trusted content providers

- Enemy:
  - 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: mitigation procedures:
  - detection
  - revocation list
Protocols

Provider-client:

1. $C \rightarrow P : \text{Request content}$
2. $C \leftrightarrow P : \text{Mutual authentication, [payment]}$
3. $P \rightarrow C : \{M\}_K, \{K\}_{pk(C)}, R, \text{metadata}(M), \Lambda$

Client-client:

1. $D \rightarrow C : \text{Request content}$
2. $C \leftrightarrow D : \text{Mutual authentication}$
3. $C \rightarrow D : \{M\}'_K, \{K\}'_{pk(D)}, R_C(M), R', \text{metadata}(M), \Lambda, \Lambda'$
4. $D : \text{Verification}$
5. $D \rightarrow C : \psi, \text{[payment]}$
Weaknesses

1. P2C: no link request — rights attack: insert rights
Weaknesses

1. P2C: no link request — rights attack: insert rights

2. C2C: No link delivery — payment attack: abort before payment
Weaknesses

1. P2C: no link request — rights attack: insert rights

2. C2C: No link delivery — payment attack: abort before payment

Fairness (violated in C2C):

"Either both parties terminate successfully, or none does"
Weaknesses

1. P2C: no link request — rights attack: insert rights

2. C2C: No link delivery — payment attack: abort before payment

Fairness (violated in C2C):

“Either both parties terminate successfully, or none does”

- Not possible without TTP
- Optimistic fair exchange: only use TTP if fairness violated otherwise
- Two protocols: optimistic exchange and recovery
Motivation:

Goals of Nuovo:
Motivation:

- address weaknesses
- increase assurance of security

Goals of Nuovo:
Motivation:

- address weaknesses
- increase assurance of security

Goals of Nuovo:

- effectiveness
- secrecy
- resist content masquerading
- fairness
P2C protocol

Introduction

NPGCT Scheme

Nuovo DRM

- Design
- P2C protocol
- C2C protocols

Assessment

Conclusions

Provider — client exchange:

1. \(\text{owner}(C) \rightarrow C: \ P, h(M), R\)
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. \(P \rightarrow C: \ \{M\}_K, \ \{K\}_{pk(C)}, \ \{R, n_C\}_{SK(P)}\)

- concrete protocol
- first weakness addressed (validity of \(R\))
C2C protocols

Client — client optimistic exchange:

1. \( \text{owner}(D) \rightarrow D : C, h(M), R' \)
2. \( D \rightarrow C : D, n_D \)
3. \( C \rightarrow D : \{n_C, n_D, D\}_{sk(C)} \)
4. \( D \rightarrow C : \{n_D, n_C, h(M), R', C\}_{sk(D)} \)
5. \( C \rightarrow D : \{M\}_K, \{K\}_{pk(D)}, \{R', n_D\}_{sk(C)} \)

Client — client, recovery:

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

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:

✓ effectiveness
✓ secrecy
✓ resisting content masquerading
  – fairness
Analysis results

Modelled scenario’s checked with CADP:

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

- goal: limit interaction with compromised devices
- method: Device Revocation List (DRL)
- trade off: size vs. security

Nuovo’s approach:
Device revocation

- goal: limit interaction with compromised devices
- method: Device Revocation List (DRL)
- trade off: size vs. security

Nuovo’s approach:

- $P$ maintains $DRL$
Device revocation

- goal: limit interaction with compromised devices
- method: Device Revocation List (DRL)
- trade off: size vs. security

Nuovo’s approach:

- $P$ maintains $DRL$
- $C$ maintains $DRL_c$ and list of friends $f_c$,
  
  \[DRL_c = L_c(s) \cup L_c(o)\]
Device revocation

- goal: limit interaction with compromised devices
- method: Device Revocation List (DRL)
- trade off: size vs. security

Nuovo’s approach:

- $P$ maintains $DRL$
- $C$ maintains $DRL_c$ and list of friends $f_c,$
  
  $$DRL_c = L_c(s) \cup L_c(o)$$

- on contact with $P$:
  
  $$L_c(s) := f_c \cap DRL; DRL_c := L_c(s) \cup L_c(o)$$
Device revocation

- goal: limit interaction with compromised devices
- method: Device Revocation List (DRL)
- trade off: size vs. security

Nuovo’s approach:

- $P$ maintains $DRL$
- $C$ maintains $DRL_c$ and list of friends $f_c$,
  \[ DRL_c = L_c(s) \cup L_c(o) \]

  on contact with $P$:
  \[ L_c(s) := f_c \cap DRL; DRL_c := L_c(s) \cup L_c(o) \]

  on contact with $D$:
  \[ L_c(o) := L_c(o) \cup L_d(s); DRL_c := L_c(s) \cup L_c(o) \]
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!