Nuovo DRM

Introducing Fair Exchange in Digital Rights Management

Hugo Jonker, Mohammad Torabi Dashti, Srijith Krishnan Nair

SaToSS group, University of Luxembourg

FM group, Eindhoven University of Technology

Digital Rights Management

- idea: trade digital “content”
- problem: unlimited, perfect copying
- generalisation: access control needed

- DRM: bundle access control with content

Requirements of DRM systems

- G1. effectiveness
- G2. secrecy
- G3. resist content masquerading
- G4. *strong fairness*

fair exchange

Alice: A $\longleftrightarrow$ Bob: B

fair exchange

Alice: A $\longleftrightarrow$ Bob: B

- Two fair endings:
  - Alice: B; Bob: A
  - Alice: A; Bob: B
- recovery protocol
- TTP needed
- *optimistic* fair exchange: TTP hardly needed

P2P exchange

Buying content c with rights r':

1. $d2 \rightarrow d1$: Request content
2. $d1 \leftrightarrow d2$: Mutual authentication
3. $d1 \rightarrow d2$: $\{c\}_{K'}, \{K'\}_{pk(d2)}, R_{d1}(c), r', \sigma, \Lambda, \Lambda'$
   $\Lambda' = \{h(d1, d2, c, \sigma, r')\}_{sk(d1)}$
4. $d2$: Verifies σ, Λ' and $R_{d1}(c)$ using Λ
5. $d2 \rightarrow d1$: $\psi, [payment]$
   $\psi = \{h(d1, P, \{c\}_{K'}, \sigma, r')\}_{sk(d2)}$

— from [NPGCT05]

NPGCT05 issues

- replay of rights
- no fairness

concept

- address NPGCT05's flaws
- verified security
- practical security

assumptions and limits

- A1. trusted devices
- A2. resilient communication
- A3. PKI hierarchy
- A4. price negotiations

fair exchange

$$
\begin{array}{lrcl}
1. & owner(d2) & \rightarrow d2: & d1,\ h(c),\ r' \\
2. & d2 & \rightarrow d1: & d2,\ n_{d2} \\
3. & d1 & \rightarrow d2: & \{n'_{d1},\ n_{d2},\ d2\}_{sk(d1)} \\
4. & d2 & \rightarrow d1: & \{n_{d2},\ n'_{d1},\ h(c),\ r',\ d1\}_{sk(d2)} \\
5. & d1 & \rightarrow d2: & \{c\}_{K'},\ \{K'\}_{pk(d2)},\ \{r',\ n_{d2}\}_{sk(d1)}
\end{array}
$$

where:

- $d1$, $d2$: devices
- $h(c)$: hash of content c
- n_x: nonce of X
- r': rights

recovery

$$
\begin{array}{lll}
1. & owner(d2) \rightarrow d2: & d1,\ h(c),\ r' \\
2. & d2 \rightarrow d1: & d2,\ n_{d2} \\
3. & d1 \rightarrow d2: & \{n'_{d1},\ n_{d2},\ d2\}_{sk(d1)} \\
4. & d2 \rightarrow d1: & \{n_{d2},\ n'_{d1},\ h(c),\ r',\ d1\}_{sk(d2)} \\
5^r. & d2: & resolves(d2)
\end{array}
$$

$$
\begin{array}{lll}
6^r. & d2 \rightarrow P: & d2,\ n'_{d2} \\
7^r. & P \rightarrow d2: & \{n'_P,\ n'_{d2},\ d2\}_{sk(P)} \\
8^r. & d2 \rightarrow P: & \{n'_{d2},\ n'_P,\ \langle n_{d2},\ n'_{d1},\ h(c),\ r',\ d1\rangle,\ r'',\ P\}_{sk(d2)} \\
9^r. & P \rightarrow d2: & \{c\}_{K''},\ \{K''\}_{pk(d2)},\ \{r'',\ n'_{d2}\}_{SK(P)}
\end{array}
$$

approach

- formalise processes in μCRL
  abstract actions highlight processing steps
- Intruder model that respects RCC
- formalise goals in regular μ-calculus
- finite model checking: limited instance
  2 scenario's.

abstract actions

- $request()$ start of exchange for receiving device
- $update()$ successful termination of exchange
- $last_{ttp}$ no more TTP available

fair exchange

$$\mathbf{d1}(\Omega, n_{d1}) =$$

$$\sum_{\substack{r \in Rgts \\ c \in Cont}} \mathbf{recv}(d2; d2, h(c), r) \cdot \mathbf{send}(d2; d1, n_{d1}) \cdot$$

$$\sum_{n \in Nonce} \mathbf{recv}(d2; \{n,\ n_{d1},\ d1\}_{sk(d2)}) \cdot \mathbf{send}(d2; \{n_{d1},\ n,\ h(c),\ r,\ d2\}_{sk(d1)}) \cdot$$

$$\mathit{request}(d1, h(c), r, d2) \cdot$$

$$\sum_{K \in Key} \mathbf{recv}(d2; \{c\}_K,\ \{K\}_{pk(d1)},\ \{r,\ n_{d1}\}_{sk(d2)}) \cdot$$

$$\mathit{update}(d1, h(c), r, d2) \cdot \mathbf{d1}(\Omega \cup \{\langle c, r \rangle\}, nxt(n_{d1}))$$

$$+ \quad \mathrm{RESOLVE}(\Omega, n_{d1}, (n_{d1},\ n,\ h(c),\ r,\ d2))$$

recovery

$$\mathrm{RESOLVE}(\Omega, n_{d1}, (n_{d1},\ n,\ h(c),\ r,\ d2)) = \mathit{resolves}(d1)\cdot$$

$$\sum_{\substack{r\in Rgts\\ c\in Cont}} \mathbf{send}(P; d1, n_{d1})\cdot$$

$$\sum_{n'\in Nonce} \mathbf{recv}(P; \{n',\ n_{d1},\ d1\}_{sk(P)})\cdot$$

$$\mathbf{send}(P; \{n_{d1},\ n',\ (n_{d1},\ n,\ h(c),\ r,\ d2),\ P\}_{sk(d1)})\cdot$$

$$\mathit{request}(d1, h(c), r, P)\cdot$$

$$\sum_{K\in Key} \mathbf{recv}(P; \{c\}_K,\ \{K\}_{pk(d1)},\ \{r,\ n_{d1}\}_{sk(P)})\cdot$$

$$\mathit{update}(d1, c, r, P)\cdot d1(\Omega\cup\{\langle c, r\rangle\}, nxt(n_{d1}))$$

intruder model

$$
\begin{aligned}
I(X,Y) = \quad & \sum_{\substack{p \in Agent \\ m \in Msg}} \mathbf{recv}(p,m,I) \cdot I(X \cup \{m\}, Y \cup \{m\}) + \\
& \sum_{\substack{p \in Agent \\ m \in Msg}} \mathbf{send}(I,m,p) \cdot I(X, Y \setminus \{m\}) \lhd m \in Y \rhd \delta + \\
& \sum_{\substack{p \in Agent \\ m \in Msg}} \mathbf{send}^{\diamond}(I,m,p) \cdot I(X,Y) \lhd m \in synth(X) \setminus Y \rhd \delta + \\
& \sum_{c \in Cont} revealed(c) \cdot \delta \lhd c \in synth(X) \rhd \delta
\end{aligned}
$$

— From [CT06]

Scenarios

- S_0: one provider P, $d1$, $d2$, trusted network, no intruder.
- S_1: three providers, $d1$, $d2$, untrusted network, intruder controls $d1$.

Both:

- content: c_1, c_2, c_3
- rights: r_1, r_2, r_1 allows resale of r_2

goals

- G1. effectiveness

$$[\mathsf{T}^* \cdot \mathit{request}(d1, c, r, P)]\ \mu X.(\langle \mathsf{T} \rangle \mathsf{T}\ \wedge\ [\neg \mathit{update}(d1, c, r, P)]X)$$

goals

- G1. effectiveness

$$[\mathsf{T}^* \cdot \mathit{request}(d1, c, r, P)]\ \mu X.(\langle \mathsf{T} \rangle \mathsf{T}\ \wedge\ [\neg \mathit{update}(d1, c, r, P)]X)$$

- G2. secrecy

$$[\mathsf{T}^* \cdot \mathit{revealed}(c)]\mathsf{F}$$

goals

- G1. effectiveness

$$[\mathsf{T}^* \cdot \mathit{request}(d1, c, r, P)]\ \mu X.(\langle\mathsf{T}\rangle\mathsf{T}\ \wedge\ [\neg \mathit{update}(d1, c, r, P)]X)$$

- G2. secrecy

$$[\mathsf{T}^* \cdot \mathit{revealed}(c)]\mathsf{F}$$

- G3. resist content masquerading

$$[(\neg \mathit{request}(d1, c, r, P))^* \cdot \mathit{update}(d1, c, r, P)]\mathsf{F}$$

fairness

- for provider
- for $d2$ when buying from provider
- for $d2$ when reselling
- *for $d2$ when buying from $d1$*

fairness

- for provider
- for $d2$ when buying from provider
- for $d2$ when reselling
- *for $d2$ when buying from $d1$*

$$[\mathsf{T}^* \cdot request(d2, c, r, d1) \cdot (\neg(resolves(d2) \vee update(d2, c, r, d1)))^*]$$
$$\langle(\neg com^{\diamond}(-,-,-))^* \cdot (resolves(d2) \vee update(d2, c, r, d1))\rangle\mathsf{T}$$

fairness

- for provider
- for $d2$ when buying from provider
- for $d2$ when reselling
- *for $d2$ when buying from $d1$*

$$[\mathsf{T}^* \cdot request(d2, c, r, d1) \cdot (\neg(resolves(d2) \vee update(d2, c, r, d1)))^*]$$
$$\langle(\neg com^{\diamond}(-,-,-))^* \cdot (resolves(d2) \vee update(d2, c, r, d1))\rangle \mathsf{T}$$

$$\wedge$$

$$[(\neg last_{ttp})^* \cdot request(d2, c, r, d1) \cdot (\neg last_{ttp})^* \cdot resolves(d2) \cdot$$
$$(\neg(update(d2, c, r, P) \vee last_{ttp}))^*]$$
$$\langle(\neg com^{\diamond}(-,-,-))^* \cdot update(d2, c, r, P)\rangle \mathsf{T}$$

results

- G1. effectiveness: √

results

- G1. effectiveness: √
- G2. secrecy: √

results

- G1. effectiveness: √
- G2. secrecy: √
- G3. resist content masquerading: √

results

- G1. effectiveness: √
- G2. secrecy: √
- G3. resist content masquerading: √
- G4. strong fairness:

results

- G1. effectiveness: √
- G2. secrecy: √
- G3. resist content masquerading: √
- G4. strong fairness:
  - for provider: √

results

- G1. effectiveness: $\surd$
- G2. secrecy: $\surd$
- G3. resist content masquerading: $\surd$
- G4. strong fairness:
  - for provider: $\surd$
  - for $d2$ when buying from provider: $\surd$

results

- G1. effectiveness: $\surd$
- G2. secrecy: $\surd$
- G3. resist content masquerading: $\surd$
- G4. strong fairness:
  - for provider: $\surd$
  - for $d2$ when buying from provider: $\surd$
  - for $d2$ when reselling: $\surd$

results

- G1. effectiveness: $\surd$
- G2. secrecy: $\surd$
- G3. resist content masquerading: $\surd$
- G4. strong fairness:
  - for provider: $\surd$
  - for $d2$ when buying from provider: $\surd$
  - for $d2$ when reselling: $\surd$
  - for $d2$ when buying from $d1$: $\surd$

final remarks

Nuovo beyond this talk:

- attention to practical security
- proof-of-concept implementation

Closing remarks:

- fair exchange in DRM seems possible
- formal modelling & verification helps
- only finite instances checked
- DRM also needs practical security (done for Nuovo)

last slide

Thank you for your attention.

Questions?