Reduction of access control decisions

Nicola Zannone
Outline

Access Decision Sets

Decision Reduction

Safe Reduction

Conclusion
Outline

Access Decision Sets

Decision Reduction

Safe Reduction

Conclusion
Access Control
Access Control
Decision Sets

- Two-valued: $D_2 = \{1, 0\}$
  - $1 = \text{Permit}$, $0 = \text{Deny}$
  - Access Matrix, HRU, Bell-LaPadula, Chinese Wall, RBAC, . . .

- Three-valued: $D_3 = \{1, 0, \perp\}$
  - $\perp = \text{not-applicable}$
  - EPAL, PTaCL (target evaluation), . . .

- Four-valued: $D_4$
  - Conflicts: $D_4 = \{\emptyset, 1, 0, \{1, 0\}\}$
  - Errors: $D_4 = \{\text{P, D, NA, I}\}$ (XACML v2/v3)

- Six-valued: $D_6 = \{\text{P, D, NA, I\{P\}, I\{D\}, I\{PD\}}\}$
  - XACML v3

- Seven-valued: $D_7 = \emptyset(D_3) \setminus \emptyset$
  - PTaCL (policy evaluation)

- Other decision sets: risk-based, . . .
Combining Operators (1)

Access Decision Sets

<table>
<thead>
<tr>
<th>□</th>
<th>1 0 ⊥</th>
<th>□</th>
<th>1 0 ⊥</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1 0 ⊥</td>
<td>1</td>
<td>1 1 ⊥</td>
</tr>
<tr>
<td>0</td>
<td>0 0 ⊥</td>
<td>0</td>
<td>1 0 ⊥</td>
</tr>
<tr>
<td>⊥</td>
<td>⊥ ⊥ ⊥</td>
<td>⊥</td>
<td>⊥ ⊥ ⊥</td>
</tr>
</tbody>
</table>

Kleene Algebra
weak conjunction (□) disjunction (□)
strong conjunction (ī) disjunction (ī)
negation (¬), weakening (\sim)

<table>
<thead>
<tr>
<th>□</th>
<th>1 0 ⊥</th>
<th>ā</th>
<th>1 0 ⊥</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1 0 ⊥</td>
<td>1</td>
<td>1 1 1</td>
</tr>
<tr>
<td>0</td>
<td>0 0 0</td>
<td>0</td>
<td>1 0 ⊥</td>
</tr>
<tr>
<td>⊥</td>
<td>⊥ 0 ⊥</td>
<td>⊥</td>
<td>1 ⊥ ⊥</td>
</tr>
</tbody>
</table>

D2: Boolean algebra

D3: Kleene algebra

D4: XACML v2/v3

- permit overrides (pov) v2
- deny overrides (dov) v2
- first applicable (fa)
- only one applicable (ooa)
- permit unless deny (pud) v3
- deny unless permit (dup) v3

<table>
<thead>
<tr>
<th>dov</th>
<th>P</th>
<th>D</th>
<th>NA</th>
<th>I{P}</th>
<th>I{D}</th>
<th>I{PD}</th>
</tr>
</thead>
<tbody>
<tr>
<td>P</td>
<td>P</td>
<td>D</td>
<td>P</td>
<td>I{PD}</td>
<td>I{PD}</td>
<td></td>
</tr>
<tr>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td></td>
</tr>
<tr>
<td>NA</td>
<td>P</td>
<td>D</td>
<td>NA</td>
<td>I{P}</td>
<td>I{D}</td>
<td>I{PD}</td>
</tr>
<tr>
<td>I{P}</td>
<td>P</td>
<td>D</td>
<td>I{P}</td>
<td>I{P}</td>
<td>I{P}</td>
<td>I{PD}</td>
</tr>
<tr>
<td>I{D}</td>
<td>I{PD}</td>
<td>D</td>
<td>I{D}</td>
<td>I{PD}</td>
<td>I{D}</td>
<td>I{PD}</td>
</tr>
<tr>
<td>I{PD}</td>
<td>I{PD}</td>
<td>D</td>
<td>I{PD}</td>
<td>I{PD}</td>
<td>I{PD}</td>
<td>I{PD}</td>
</tr>
</tbody>
</table>

D6: XACML v3

- permit overrides (pov)
- deny overrides (dov)
Combining Operators (2)

\( \mathcal{D}_7 \): operators over \( \mathcal{D}_3 \) extended point-wise

\[ \overline{\text{op}}(X, Y) = \{ \text{op}(x, y) \mid x \in X \land y \in Y \} \]
**Exercise**

Define strong disjunctions ($\tilde{\sqcup}$) in $\mathcal{D}_7$

<table>
<thead>
<tr>
<th>$\tilde{\sqcup}$</th>
<th>1</th>
<th>0</th>
<th>$\perp$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>$\perp$</td>
</tr>
<tr>
<td>$\perp$</td>
<td>1</td>
<td>$\perp$</td>
<td>$\perp$</td>
</tr>
</tbody>
</table>
Define strong disjunctions (\(\tilde{\lor}\)) in \(\mathcal{D}_7\)

<table>
<thead>
<tr>
<th>(\tilde{\lor})</th>
<th>1</th>
<th>0</th>
<th>(\bot)</th>
<th>1, (\bot)</th>
<th>0, (\bot)</th>
<th>1, 0</th>
<th>1, 0, (\bot)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>(\bot)</td>
<td>1, (\bot)</td>
<td>0, (\bot)</td>
<td>1, 0</td>
<td>1, 0, (\bot)</td>
</tr>
<tr>
<td>(\bot)</td>
<td>1</td>
<td>(\bot)</td>
<td>(\bot)</td>
<td>1, (\bot)</td>
<td>(\bot)</td>
<td>1, (\bot)</td>
<td>1, (\bot)</td>
</tr>
<tr>
<td>1, (\bot)</td>
<td>1</td>
<td>1, (\bot)</td>
<td>1, (\bot)</td>
<td>1, (\bot)</td>
<td>1, (\bot)</td>
<td>1, (\bot)</td>
<td>1, (\bot)</td>
</tr>
<tr>
<td>0, (\bot)</td>
<td>1</td>
<td>0, (\bot)</td>
<td>(\bot)</td>
<td>1, (\bot)</td>
<td>0, (\bot)</td>
<td>1, 0, (\bot)</td>
<td>1, 0, (\bot)</td>
</tr>
<tr>
<td>1, 0</td>
<td>1</td>
<td>1, 0</td>
<td>1, (\bot)</td>
<td>1, (\bot)</td>
<td>1, 0, (\bot)</td>
<td>1, 0</td>
<td>1, 0, (\bot)</td>
</tr>
<tr>
<td>1, 0, (\bot)</td>
<td>1</td>
<td>1, 0, (\bot)</td>
<td>1, (\bot)</td>
<td>1, (\bot)</td>
<td>1, 0, (\bot)</td>
<td>1, 0</td>
<td>1, 0, (\bot)</td>
</tr>
</tbody>
</table>
Outline

Access Decision Sets

Decision Reduction

Safe Reduction

Conclusion
Reducing decision sets

- Deal with non-conclusive decisions
- Ensure compatibility of operators when language evolves over time
  - e.g. from XACML v2 to XACML v3
- Reuse operators over smaller decision sets
- Enable interoperability between systems
A decision reduction maps a decision set into a smaller decision set by mapping all decisions of a set to decisions of a subset, while leaving the decisions in the subset unchanged.
Sample Reductions

\( \rho_{32} : \mathcal{D}_3 \rightarrow \mathcal{D}_2 \)

\( \mathcal{D}_3 = \{1, 0, \bot\} \)
\( \mathcal{D}_2 = \{1, 0\} \)

\( \rho_{32}^1(d) = \begin{cases} 
    d & \text{if } d \in \{1, 0\} \\
    1 & \text{if } d = \bot 
\end{cases} \)

\( \rho_{32}^0(d) = \begin{cases} 
    d & \text{if } d \in \{1, 0\} \\
    0 & \text{if } d = \bot 
\end{cases} \)

\( \rho_{64} : \mathcal{D}_6 \rightarrow \mathcal{D}_4 \) (XACML v3; XACML v3 to XACML v2)

\( \mathcal{D}_6 = \{P, D, NA, I\{P\}, I\{D\}, I\{PD\}\} \)
\( \mathcal{D}_4 = \{P, D, NA, I\} \)

\( \rho_{64}^1(d) = \begin{cases} 
    d & \text{if } d \in \{P, D, NA\} \\
    1 & \text{if } d \in \{I\{P\}, I\{D\}, I\{PD\}\} 
\end{cases} \)

\( \rho_{64}^0(d) = \begin{cases} 
    d & \text{if } d \in \{P, D, NA\} \\
    0 & \text{if } d \in \{I\{P\}, I\{D\}, I\{PD\}\} 
\end{cases} \)  \textbf{Note: } I \cong I\{PD\}

\( \rho_{76} : \mathcal{D}_7 \rightarrow \mathcal{D}_6 \) (PTaCL to XACML v3)

\( \mathcal{D}_7 = \wp(\mathcal{D}_3) \setminus \emptyset \)

\( \rho_{76}^1(d) = \begin{cases} 
    \{1\} & = P \\
    \{0\} & = D \\
    \{\bot\} & = NA \\
    \{1, \bot\} & = I\{P\} \\
    \{0, \bot\} & = I\{D\} \\
    \{1, 0\}, \{1, 0, \bot\} & = I\{PD\} 
\end{cases} \)
Example

Reduce strong disjunction ($\tilde{\lor}$) defined over $D_7$ into $D_6$ (XACML v3)

$D_6 = \{P, D, NA, I\{P\}, I\{D\}, I\{PD\}\}$

$D_7 = \varnothing(D_3) \setminus \emptyset$

$\rho_{76}^1(\{1, 0, \perp\}) = \rho_{76}^1(\{1, 0\}) = I\{PD\}$
Problem solved?
Example 1: XACML v3

$fa, pud, dup, ooa: \mathcal{D}_4 = \{P, D, NA, I\}$

$dov, pov: \mathcal{D}_6 = \{P, D, NA, I\{P\}, I\{D\}, I\{PD\}\}$
Example 1: XACML v3

fa, pud, dup, ooa: \( D_4 = \{P, D, NA, I\} \)
dov, pov: \( D_6 = \{P, D, NA, I\{P\}, I\{D\}, I\{PD\}\} \)
Example 1: XACML v3

\[ \text{fa, pud, dup, ooa: } D_4 = \{P, D, NA, I\} \]
\[ \text{dov, pov: } D_6 = \{P, D, NA, I\{P\}, I\{D\}, I\{PD\}\} \]

\[ \rho_{64}(I\{P\}) = I \]
Example 1: XACML v3

fa, pud, dup, ooa: $\mathcal{D}_4 = \{P, D, NA, I\}$
dov, pov: $\mathcal{D}_6 = \{P, D, NA, I\{P\}, I\{D\}, I\{PD\}\}$

\[\rho_{64}(I\{P\}) = I\]

\[fa(I, P) = I\]
Example 1: XACML v3

fa, pud, dup, ooa: $\mathcal{D}_4 = \{P, D, NA, I\}$
dov, pov: $\mathcal{D}_6 = \{P, D, NA, I\{P\}, I\{D\}, I\{PD\}\}$

\[\rho_{64}(I\{P\}) = I\]
\[fa(I, P) = I\]
\[(I \cong I\{PD\})\]
Example 1: XACML v3

fa, pud, dup, ooa: \( D_4 = \{P, D, NA, I\} \)
dov, pov: \( D_6 = \{P, D, NA, I\{P\}, I\{D\}, I\{PD\}\} \)

\[ \rho_{64}(I\{P\}) = I \]
\[ fa(I, P) = I \]
\[ (I \cong I\{PD\}) \]
\[ dov(I\{PD\}, P) = I\{PD\} \]
Example 1: XACML v3

fa, pud, dup, ooa: \( \mathcal{D}_4 = \{P, D, NA, I\} \)
dov, pov: \( \mathcal{D}_6 = \{P, D, NA, I\{P\}, I\{D\}, I\{PD\}\} \)

\[
\rho_{64}(I\{P\}) = I \\
fa(I, P) = I \\
(I \cong I\{PD\}) \\
dov(I\{PD\}, P) = I\{PD\} \\
(I\{PD\} \cong I)
\]
Example 1: XACML v3

\( \mathcal{D}_4 = \{ P, D, NA, I \} \)
\( \mathcal{D}_6 = \{ P, D, NA, I\{P\}, I\{D\}, I\{PD\} \} \)

\[ \rho_{64}(I\{P\}) = I \]
\[ \text{fa}(I, P) = I \]
\[ (I \equiv I\{PD\}) \]
\[ \text{dov}(I\{PD\}, P) = I\{PD\} \]
\[ (I\{PD\} \equiv I) \]
Example 1: XACML v3

\[ \mathcal{D}_4 = \{ P, D, NA, I \} \]  
\[ \mathcal{D}_6 = \{ P, D, NA, I\{P\}, I\{D\}, I\{PD\} \} \]

\[ \rho_{64}(I\{P\}) = I \]  
\[ fa(I, P) = I \]  
\[ (I \cong I\{PD\}) \]  
\[ dov(I\{PD\}, P) = I\{PD\} \]  
\[ (I\{PD\} \cong I) \]

\[ fa'(I\{P\}, P) = I\{P\} \]
Example 1: XACML v3

\( fa, pud, dup, ooa: \mathcal{D}_4 = \{P, D, NA, I\} \)

\( dov, pov: \mathcal{D}_6 = \{P, D, NA, I\{P\}, I\{D\}, I\{PD\}\} \)

\[ \rho_{64}(I\{P\}) = I \]
\[ fa(I, P) = I \]
\[ (I \cong I\{PD\}) \]
\[ dov(I\{PD\}, P) = I\{PD\} \]
\[ (I\{PD\} \cong I) \]

\[ fa'(I\{P\}, P) = I\{P\} \]
\[ dov(I\{P\}, P) = P \]
Example 2: From XACML v3 to XACML v2

<table>
<thead>
<tr>
<th>dov</th>
<th>P</th>
<th>D</th>
<th>NA</th>
<th>I{P}</th>
<th>I{D}</th>
<th>I{PD}</th>
</tr>
</thead>
<tbody>
<tr>
<td>P</td>
<td>P</td>
<td>D</td>
<td>P</td>
<td>P</td>
<td>I{PD}</td>
<td>I{PD}</td>
</tr>
<tr>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>NA</td>
<td>P</td>
<td>D</td>
<td>NA</td>
<td>I{P}</td>
<td>I{D}</td>
<td>I{PD}</td>
</tr>
<tr>
<td>I{P}</td>
<td>P</td>
<td>D</td>
<td>I{P}</td>
<td>I{P}</td>
<td>I{PD}</td>
<td>I{PD}</td>
</tr>
<tr>
<td>I{D}</td>
<td>I{PD}</td>
<td>D</td>
<td>I{D}</td>
<td>I{PD}</td>
<td>I{D}</td>
<td>I{PD}</td>
</tr>
<tr>
<td>I{PD}</td>
<td>I{PD}</td>
<td>D</td>
<td>I{PD}</td>
<td>I{PD}</td>
<td>I{PD}</td>
<td>I{PD}</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>dov</th>
<th>P</th>
<th>D</th>
<th>NA</th>
<th>I</th>
</tr>
</thead>
<tbody>
<tr>
<td>P</td>
<td>P</td>
<td>D</td>
<td>P</td>
<td>D</td>
</tr>
<tr>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>NA</td>
<td>P</td>
<td>D</td>
<td>NA</td>
<td>D</td>
</tr>
<tr>
<td>I</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
</tbody>
</table>

**Note:** In XACML v2 there are two variants of deny-overrides: one variant for rules and one for policies (above)
Example 2: From XACML v3 to XACML v2

\[
\text{dov}(I\{P\}, P) = P \\
\text{dov}(I\{D\}, P) = I\{PD\} \\
\text{dov}(I\{PD\}, P) = I\{PD\}
\]

\[
\text{dov}(I, P) = D
\]
Example 2: From XACML v3 to XACML v2

\[
\begin{align*}
dov(I\{P\}, P) &= P \\
dov(I\{D\}, P) &= I\{PD\} \\
dov(I\{PD\}, P) &= I\{PD\}
\end{align*}
\]

\[
\begin{align*}
dov(I, P) &= D
\end{align*}
\]

B has to evaluate expression $dov(I\{P\}, P)$ based on the partial decisions of A.
Example 2: From XACML v3 to XACML v2

\[ \text{dov}(I\{P\}, P) = P \]
\[ \text{dov}(I\{D\}, P) = I\{PD\} \]
\[ \text{dov}(I\{PD\}, P) = I\{PD\} \]

\[ \text{dov}(I, P) = D \]

\( B \) has to evaluate expression \( \text{dov}(I\{P\}, P) \) based on the partial decisions of \( A \)

**Case 1:** \( \text{dov} \) is computed by \( A \)

**Case 2:** \( \text{dov} \) is computed by \( B \)
Example 2: From XACML v3 to XACML v2

\[
\begin{align*}
\text{dov}(I\{P\}, P) &= P \\
\text{dov}(I\{D\}, P) &= I\{PD\} \\
\text{dov}(I\{PD\}, P) &= I\{PD\}
\end{align*}
\]

\[\text{dov}(I, P) = D\]

\(B\) has to evaluate expression \(\text{dov}(I\{P\}, P)\) based on the partial decisions of \(A\)

**Case 1:** dov is computed by \(A\)
\(A : \text{dov}(I\{P\}, P) = P\)

**Case 2:** dov is computed by \(B\)
Example 2: From XACML v3 to XACML v2

\[
\begin{align*}
\text{dov}(I\{P\}, P) &= P \\
\text{dov}(I\{D\}, P) &= I\{PD\} \\
\text{dov}(I\{PD\}, P) &= I\{PD\}
\end{align*}
\]

\(B\) has to evaluate expression \(\text{dov}(I\{P\}, P)\) based on the partial decisions of \(A\)

**Case 1:** dov is computed by \(A\)

\(A\) : \(\text{dov}(I\{P\}, P) = P\)

\(A \rightarrow B\) : \(P\)

**Case 2:** dov is computed by \(B\)
Example 2: From XACML v3 to XACML v2

\[
\begin{align*}
\text{dov}(I\{P\}, P) &= P \\
\text{dov}(I\{D\}, P) &= I\{PD\} \\
\text{dov}(I\{PD\}, P) &= I\{PD\}
\end{align*}
\]

\(B\) has to evaluate expression \(\text{dov}(I\{P\}, P)\) based on the partial decisions of \(A\)

**Case 1:** \(\text{dov}\) is computed by \(A\)

\[
\begin{align*}
A & : \text{dov}(I\{P\}, P) = P \\
A \to B & : P \\
B & : P \leftrightarrow P
\end{align*}
\]

**Case 2:** \(\text{dov}\) is computed by \(B\)

\[
\begin{align*}
\text{dov}(I, P) &= D
\end{align*}
\]
Example 2: From XACML v3 to XACML v2

\[
dov(I\{P\}, P) = P
\]
\[
dov(I\{D\}, P) = I\{PD\}
\]
\[
dov(I\{PD\}, P) = I\{PD\}
\]

\(B\) has to evaluate expression \(dov(I\{P\}, P)\) based on the partial decisions of \(A\)

**Case 1:** \(dov\) is computed by \(A\)

\[
A : dov(I\{P\}, P) = P
\]
\[
A \rightarrow B : P
\]
\[
B : P \mapsto P
\]

**Case 2:** \(dov\) is computed by \(B\)

\[
A \rightarrow B : I\{P\}, P
\]
Example 2: From XACML v3 to XACML v2

\[ \text{dov}(I\{ \{P\} \}, P) = P \]
\[ \text{dov}(I\{ \{D\} \}, P) = I\{ \{PD\} \} \]
\[ \text{dov}(I\{ \{PD\} \}, P) = I\{ \{PD\} \} \]

\(B\) has to evaluate expression \(\text{dov}(I\{\{P\}\}, P)\) based on the partial decisions of \(A\)

**Case 1:** \(\text{dov}\) is computed by \(A\)
- \(A\) : \(\text{dov}(I\{\{P\}\}, P) = P\)
- \(A \rightarrow B\) : \(P\)
- \(B\) : \(P \rightarrow P\)

**Case 2:** \(\text{dov}\) is computed by \(B\)
- \(A \rightarrow B\) : \(I\{\{P\}\}, P\)
- \(B\) : \(I\{\{P\}\} \leftrightarrow I, P \leftrightarrow P\)
Example 2: From XACML v3 to XACML v2

\[
\begin{align*}
dov(I\{P\}, P) &= P \\
dov(I\{D\}, P) &= I\{PD\} \\
dov(I\{PD\}, P) &= I\{PD\}
\end{align*}
\]

\(B\) has to evaluate expression \(dov(I\{P\}, P)\) based on the partial decisions of \(A\)

**Case 1:** \(dov\) is computed by \(A\)

\[
\begin{array}{l}
A \quad : \\
A \to B \\
B
\end{array}
\]

\[
\begin{array}{l}
dov(I\{P\}, P) = P \\
P \\
P 
\end{array}
\]

**Case 2:** \(dov\) is computed by \(B\)

\[
\begin{array}{l}
A \to B \\
B \\
B
\end{array}
\]

\[
\begin{array}{l}
I\{P\}, P \\
I\{P\} \mapsto I, P \mapsto P \\
dov(I, P) = D
\end{array}
\]
Example 3: From PTaCL to XACML v3

Reuse weak conjunction ($\sqcap$) in XACML v3

$D_6 = \{P, D, NA, I\{P\}, I\{D\}, I\{PD\}\}$

$D_7 = \emptyset(D_3) \setminus \emptyset$

$\rho^I_{76}(\{1, 0, \perp\}) = \rho^I_{76}(\{1, 0\}) = I\{PD\}$
Example 3: From PTaCL to XACML v3

Reuse weak conjunction ($\sqcap$) in XACML v3

\[ D_6 = \{P, D, NA, I\{P\}, I\{D\}, I\{PD\}\} \]
\[ D_7 = \wp(D_3) \setminus \emptyset \]
\[ \rho_{76}^\downarrow(\{1, 0, \bot\}) = \rho_{76}^\downarrow(\{1, 0\}) = I\{PD\} \]

<table>
<thead>
<tr>
<th>$\sqcap$</th>
<th>1</th>
<th>0</th>
<th>1, \bot</th>
<th>0, \bot</th>
<th>1, 0</th>
<th>1, 0, \bot</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1, \bot</td>
<td>0, \bot</td>
<td>1, 0</td>
<td>1, 0, \bot</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0, \bot</td>
<td>0, \bot</td>
<td>0, \bot</td>
<td>0, \bot</td>
</tr>
<tr>
<td>\bot</td>
<td>\bot</td>
<td>\bot</td>
<td>\bot</td>
<td>\bot</td>
<td>\bot</td>
<td>\bot</td>
</tr>
<tr>
<td>1, \bot</td>
<td>1, \bot</td>
<td>1, \bot</td>
<td>1, 0, \bot</td>
<td>1, 0, \bot</td>
<td>1, 0, \bot</td>
<td>1, 0, \bot</td>
</tr>
<tr>
<td>0, \bot</td>
<td>0, \bot</td>
<td>0, \bot</td>
<td>0, \bot</td>
<td>0, \bot</td>
<td>0, \bot</td>
<td>0, \bot</td>
</tr>
<tr>
<td>1, 0</td>
<td>1, 0</td>
<td>1, 0, \bot</td>
<td>1, 0, \bot</td>
<td>1, 0, \bot</td>
<td>1, 0, \bot</td>
<td>1, 0, \bot</td>
</tr>
<tr>
<td>1, 0, \bot</td>
<td>1, 0, \bot</td>
<td>1, 0, \bot</td>
<td>1, 0, \bot</td>
<td>1, 0, \bot</td>
<td>1, 0, \bot</td>
<td>1, 0, \bot</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$\sqcap$</th>
<th>P</th>
<th>D</th>
<th>NA</th>
<th>I{P}</th>
<th>I{D}</th>
<th>I{PD}</th>
</tr>
</thead>
<tbody>
<tr>
<td>P</td>
<td>P</td>
<td>D</td>
<td>NA</td>
<td>I{P}</td>
<td>I{D}</td>
<td>I{PD}</td>
</tr>
<tr>
<td>D</td>
<td>D</td>
<td>D</td>
<td>NA</td>
<td>I{D}</td>
<td>I{D}</td>
<td>D, I{D}</td>
</tr>
<tr>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>I{D}</td>
<td>I{D}</td>
<td>I{PD}</td>
</tr>
<tr>
<td>I{P}</td>
<td>I{P}</td>
<td>I{D}</td>
<td>NA</td>
<td>I{P}</td>
<td>I{D}</td>
<td>I{PD}</td>
</tr>
<tr>
<td>I{D}</td>
<td>I{D}</td>
<td>I{D}</td>
<td>I{P}</td>
<td>I{D}</td>
<td>I{D}</td>
<td>I{PD}</td>
</tr>
<tr>
<td>I{PD}</td>
<td>I{PD}</td>
<td>D, I{D}</td>
<td>NA</td>
<td>I{PD}</td>
<td>I{D}</td>
<td>I{PD}</td>
</tr>
</tbody>
</table>
Example 3: From PTaCL to XACML v3

Reuse weak conjunction (⊔) in XACML v3

\[ D_6 = \{ P, D, NA, \{ P \}, \{ D \}, \{ PD \} \} \]
\[ D_7 = \varnothing(D_3) \setminus \emptyset \]
\[ \rho_{76}(\{1, 0, \perp\}) = \rho_{76}(\{1, 0\}) = \{ PD \} \]

<table>
<thead>
<tr>
<th>⊓</th>
<th>1</th>
<th>0</th>
<th>⊥</th>
<th>1, ⊥</th>
<th>0, ⊥</th>
<th>1, 0</th>
<th>1, 0, ⊥</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>⊥</td>
<td>1, ⊥</td>
<td>0, ⊥</td>
<td>1, 0</td>
<td>1, 0, ⊥</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>⊥</td>
<td>0, ⊥</td>
<td>0, ⊥</td>
<td>0</td>
<td>0, ⊥</td>
</tr>
<tr>
<td>⊥</td>
<td>⊥</td>
<td>⊥</td>
<td>⊥</td>
<td>⊥</td>
<td>⊥</td>
<td>⊥</td>
<td>⊥</td>
</tr>
<tr>
<td>1, ⊥</td>
<td>1, ⊥</td>
<td>0, ⊥</td>
<td>1, ⊥</td>
<td>0, ⊥</td>
<td>1, 0, ⊥</td>
<td>1, 0, ⊥</td>
<td></td>
</tr>
<tr>
<td>0, ⊥</td>
<td>0, ⊥</td>
<td>0, ⊥</td>
<td>0, ⊥</td>
<td>0, ⊥</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1, 0</td>
<td>1, 0</td>
<td>0</td>
<td>1, 0</td>
<td>0</td>
<td>1, 0</td>
<td>1, 0</td>
<td></td>
</tr>
<tr>
<td>1, 0, ⊥</td>
<td>1, 0, ⊥</td>
<td>0, ⊥</td>
<td>1, 0, ⊥</td>
<td>0, ⊥</td>
<td>1, 0, ⊥</td>
<td>1, 0, ⊥</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>⊓</th>
<th>P</th>
<th>D</th>
<th>NA</th>
<th>{ P }</th>
<th>{ D }</th>
<th>{ PD }</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>P</td>
<td>P</td>
<td>D</td>
<td>NA</td>
<td>{ P }</td>
<td>{ D }</td>
</tr>
<tr>
<td>0</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>NA</td>
<td>{ D }</td>
<td>{ D }</td>
</tr>
<tr>
<td>⊥</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>1, ⊥</td>
<td>{ P }</td>
<td>{ P }</td>
<td>{ D }</td>
<td>NA</td>
<td>{ P }</td>
<td>{ D }</td>
</tr>
<tr>
<td>0, ⊥</td>
<td>{ D }</td>
<td>{ D }</td>
<td>{ D }</td>
<td>NA</td>
<td>{ D }</td>
<td>{ D }</td>
</tr>
<tr>
<td>1, 0</td>
<td>{ D }</td>
<td>{ D }</td>
<td>{ D }</td>
<td>NA</td>
<td>{ D }</td>
<td>{ D }</td>
</tr>
<tr>
<td>1, 0, ⊥</td>
<td>{ PD }</td>
<td>{ PD }</td>
<td>{ D }</td>
<td>NA</td>
<td>{ PD }</td>
<td>{ D }</td>
</tr>
</tbody>
</table>
Outline

Access Decision Sets

Decision Reduction

Safe Reduction

Conclusion
How to ensure that a reduction can be performed at any level of policy composition without changing the final decision?
Safe Reduction

A reduction $\rho : D_n \rightarrow D_m$ is safe with respect to an operator $\boxtimes$ if and only if

$$\forall d_i, d_j \in D_n \quad \rho(d_i \boxtimes d_j) = \rho(d_i) \boxtimes \rho(d_j)$$

$\rho^1_{32} : D_3 \rightarrow D_2$
- $\rho^1_{32}(\bot) = 1$
- $\rho^1_{32}(d) = d$ for $d \in \{0, 1\}$

$\rho^0_{32} : D_3 \rightarrow D_2$
- $\rho^0_{32}(\bot) = 0$
- $\rho^0_{32}(d) = d$ for $d \in \{0, 1\}$

<table>
<thead>
<tr>
<th></th>
<th>$\sqcap$</th>
<th>$\sqcup$</th>
<th>$\sim$</th>
<th>$\tilde{\sqcap}$</th>
<th>$\sim$</th>
<th>$\sim$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\rho^1_{32}$</td>
<td>$\times$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
<td>$\times$</td>
<td>$\times$</td>
</tr>
<tr>
<td>$\rho^0_{32}$</td>
<td>$\checkmark$</td>
<td>$\times$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
<td>$\times$</td>
<td>$\checkmark$</td>
</tr>
</tbody>
</table>

$\rho^1_{32}(0 \sqcap \bot) = \rho^1_{32}(\bot) = 1$  \hspace{1em} vs.  \hspace{1em} $\rho^1_{32}(0) \sqcap \rho^1_{32}(\bot) = 0 \sqcap 1 = 0$

$\rho^0_{32}(1 \sqcup \bot) = \rho^0_{32}(\bot) = 0$  \hspace{1em} vs.  \hspace{1em} $\rho^0_{32}(1) \sqcup \rho^0_{32}(\bot) = 1 \sqcup 0 = 1$
Safety of Operator Composition

Access control models provide more than one operator for combining decisions

<table>
<thead>
<tr>
<th></th>
<th>∩</th>
<th>∪</th>
<th>¬</th>
<th>⊓</th>
<th>⊔</th>
<th>¬</th>
<th>¬</th>
</tr>
</thead>
<tbody>
<tr>
<td>ρ₁₃₂</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>ρ₀₃₂</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Safety condition: Given operators γ₁, . . . , γₖ : Dⁿ → Dⁿ, and a reduction ρ : Dⁿ → Dₘ, if ρ is safe for γ₁, . . . , γₖ, then ρ is safe for any combination of γ₁, . . . , γₖ.
Safety of Reduction Compositions

Reductions can be composed together to reduce further a decision set

\[ \mathcal{D}_4 \xrightarrow{\rho_{43}} \mathcal{D}_3 \xrightarrow{\rho_{32}} \mathcal{D}_2 \]

**Safety condition:** If two reductions \( \rho_1 : \mathcal{D}_m \rightarrow \mathcal{D}_n \) and \( \rho_2 : \mathcal{D}_n \rightarrow \mathcal{D}_p \) are safe for an operator \( \gamma \), then their composition \( \rho_2 \circ \rho_1 \) is also safe for \( \gamma \).

**Note:** Sufficient but not necessary condition!!
Safety Analysis of XACML v3

\[ \mathcal{D}_4 = \{P, D, NA, I\} \]
\[ \mathcal{D}_6 = \{P, D, NA, I\{P\}, I\{D\}, I\{PD\}\} \]

\[ \rho_{64} \quad \text{s.t.} \quad \begin{align*}
\rho_{64}^I(I\{P\}) &= 1 \\
\rho_{64}^I(I\{D\}) &= 1 \\
\rho_{64}^I(I\{PD\}) &= 1
\end{align*} \]

1. Is XACML v3 safe?
2. What is the most appropriate decision set for XACML v3?
3. ... also when XACML v3 is extended with new operators!!
The reduction used in XACML v3 is NOT safe!!

\[
\begin{array}{cccccccc}
\text{dov} & P & D & NA & I\{P\} & I\{D\} & I\{PD\} \\
P & P & D & P & P & I\{PD\} & I\{PD\} \\
D & D & D & D & D & D & D \\
NA & P & D & NA & I\{P\} & I\{D\} & I\{PD\} \\
I\{P\} & P & D & I\{P\} & I\{P\} & I\{PD\} & I\{PD\} \\
I\{D\} & I\{PD\} & D & I\{D\} & I\{PD\} & I\{PD\} & I\{PD\} \\
I\{PD\} & I\{PD\} & D & I\{PD\} & I\{PD\} & I\{PD\} & I\{PD\} \\
\rho_64 & \times & ✓ & ✓ & ✓ & ✓ & ✓ \\
\end{array}
\]

\[
\begin{array}{cccccccc}
\text{pov} & P & D & NA & I\{P\} & I\{D\} & I\{PD\} \\
P & P & P & P & P & P & P \\
D & P & D & D & D & I\{PD\} & D & I\{PD\} \\
NA & P & D & NA & I\{P\} & I\{D\} & I\{PD\} \\
I\{P\} & P & I\{PD\} & I\{P\} & I\{P\} & I\{PD\} & I\{PD\} \\
I\{D\} & P & D & I\{D\} & I\{PD\} & I\{PD\} & I\{PD\} \\
I\{PD\} & P & I\{PD\} & I\{PD\} & I\{PD\} & I\{PD\} & I\{PD\} \\
\rho_64 & ✓ & \times & ✓ & ✓ & ✓ & ✓ \\
\end{array}
\]

\[\rho_64(\text{dov}(P, I\{P\})) = P\]
\[\text{dov}(\rho_64(P), \rho_64(I\{P\})) = I\{PD\}\]
\[\rho_64(\text{pov}(D, I\{D\})) = D\]
\[\text{pov}(\rho_64(D), \rho_64(I\{D\})) = I\{PD\}\]
Safety Analysis of XACML v3 (2,3)

Extend XACML with PTaCL operators

Define all operators over $D_6$ and $D_7$
Redefine operators

When redefining an operator on a larger set

- Semantics undefined for certain values
- Different alternatives are possible

- `dup`, `pud`, `fa`: intuitive definition
- `pov`, `dov`, `fa`: point-wise from \( D_3 \)
- `ooa`: conservative approach
- `oooa`: record decision(s)
- \( \sqcap, \sqcup, \tilde{\sqcap}, \tilde{\sqcup} \): already defined over \( D_7 \)
Example: First applicable

<table>
<thead>
<tr>
<th>fa</th>
<th>1</th>
<th>0</th>
<th>↓</th>
<th>1, ↓</th>
<th>0, ↓</th>
<th>1, 0</th>
<th>1, 0, ↓</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>↓</td>
<td>1</td>
<td>0</td>
<td>↓</td>
<td>1, ↓</td>
<td>0</td>
<td>1, 0</td>
<td>1, 0</td>
</tr>
<tr>
<td>1, ↓</td>
<td>1, ↓</td>
<td>1, ↓</td>
<td>1, ↓</td>
<td>1, ↓</td>
<td>1, ↓</td>
<td>1, 0, ↓</td>
<td>1, 0, ↓</td>
</tr>
<tr>
<td>0, ↓</td>
<td>0, ↓</td>
<td>0, ↓</td>
<td>0, ↓</td>
<td>0, ↓</td>
<td>0, ↓</td>
<td>0, 0, ↓</td>
<td>0, 0, ↓</td>
</tr>
<tr>
<td>1, 0</td>
<td>1, 0</td>
<td>1, 0</td>
<td>1, 0</td>
<td>1, 0</td>
<td>1, 0</td>
<td>1, 0</td>
<td>1, 0</td>
</tr>
<tr>
<td>1, 0, ↓</td>
<td>1, 0, ↓</td>
<td>1, 0, ↓</td>
<td>1, 0, ↓</td>
<td>1, 0, ↓</td>
<td>1, 0, ↓</td>
<td>1, 0, ↓</td>
<td>1, 0, ↓</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(\overline{fa})</th>
<th>1</th>
<th>0</th>
<th>↓</th>
<th>1, ↓</th>
<th>0, ↓</th>
<th>1, 0</th>
<th>1, 0, ↓</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>↓</td>
<td>1</td>
<td>0</td>
<td>↓</td>
<td>1, ↓</td>
<td>0</td>
<td>1, 0</td>
<td>1, 0</td>
</tr>
<tr>
<td>1, ↓</td>
<td>1</td>
<td>1, 0</td>
<td>1, ↓</td>
<td>1, ↓</td>
<td>1, 0, ↓</td>
<td>1, 0, ↓</td>
<td>1, 0, ↓</td>
</tr>
<tr>
<td>0, ↓</td>
<td>0, ↓</td>
<td>0, ↓</td>
<td>0, ↓</td>
<td>0, ↓</td>
<td>0, ↓</td>
<td>0, 0, ↓</td>
<td>0, 0, ↓</td>
</tr>
<tr>
<td>1, 0</td>
<td>1, 0</td>
<td>1, 0</td>
<td>1, 0</td>
<td>1, 0</td>
<td>1, 0</td>
<td>1, 0</td>
<td>1, 0</td>
</tr>
<tr>
<td>1, 0, ↓</td>
<td>1, 0, ↓</td>
<td>1, 0, ↓</td>
<td>1, 0, ↓</td>
<td>1, 0, ↓</td>
<td>1, 0, ↓</td>
<td>1, 0, ↓</td>
<td>1, 0, ↓</td>
</tr>
</tbody>
</table>
Example: Only one applicable

<table>
<thead>
<tr>
<th>ooa</th>
<th>P</th>
<th>D</th>
<th>NA</th>
<th>I</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1, ⊥</td>
<td>1, 0, ⊥</td>
<td>1</td>
<td>1, 0, ⊥</td>
</tr>
<tr>
<td>0</td>
<td>1, 0, ⊥</td>
<td>1, 0, ⊥</td>
<td>0</td>
<td>1, 0, ⊥</td>
</tr>
<tr>
<td>⊥</td>
<td>1</td>
<td>0</td>
<td>⊥</td>
<td>1, 0, ⊥</td>
</tr>
<tr>
<td>1, ⊥</td>
<td>1, 0, ⊥</td>
<td>1, 0, ⊥</td>
<td>1, 0, ⊥</td>
<td>1, 0, ⊥</td>
</tr>
<tr>
<td>0, ⊥</td>
<td>1, 0, ⊥</td>
<td>1, 0, ⊥</td>
<td>1, 0, ⊥</td>
<td>1, 0, ⊥</td>
</tr>
<tr>
<td>1, 0</td>
<td>1, 0, ⊥</td>
<td>1, 0, ⊥</td>
<td>1, 0, ⊥</td>
<td>1, 0, ⊥</td>
</tr>
<tr>
<td>1, 0, ⊥</td>
<td>1, 0, ⊥</td>
<td>1, 0, ⊥</td>
<td>1, 0, ⊥</td>
<td>1, 0, ⊥</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ooa</th>
<th>P</th>
<th>D</th>
<th>NA</th>
<th>I</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1, ⊥</td>
<td>1, 0, ⊥</td>
<td>1</td>
<td>1, 0, ⊥</td>
</tr>
<tr>
<td>0</td>
<td>1, 0, ⊥</td>
<td>0, ⊥</td>
<td>0</td>
<td>1, 0, ⊥</td>
</tr>
<tr>
<td>⊥</td>
<td>1</td>
<td>0</td>
<td>⊥</td>
<td>1, 0, ⊥</td>
</tr>
<tr>
<td>1, ⊥</td>
<td>1, ⊥</td>
<td>1, 0, ⊥</td>
<td>1, ⊥</td>
<td>1, ⊥</td>
</tr>
<tr>
<td>0, ⊥</td>
<td>1, 0, ⊥</td>
<td>0, ⊥</td>
<td>0, ⊥</td>
<td>0, ⊥</td>
</tr>
<tr>
<td>1, 0</td>
<td>1, 0, ⊥</td>
<td>1, 0, ⊥</td>
<td>1, 0, ⊥</td>
<td>1, 0, ⊥</td>
</tr>
<tr>
<td>1, 0, ⊥</td>
<td>1, 0, ⊥</td>
<td>1, 0, ⊥</td>
<td>1, 0, ⊥</td>
<td>1, 0, ⊥</td>
</tr>
</tbody>
</table>
## Safety Analysis of XACML v3 (2,3)

<table>
<thead>
<tr>
<th></th>
<th>pov</th>
<th>dov</th>
<th>fa</th>
<th>dup</th>
<th>pud</th>
<th>ooa</th>
<th>ooa</th>
<th>fa</th>
<th>□</th>
<th>□</th>
<th>Ṋ</th>
<th>Ṇ</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\rho^I_{76}$</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>$\rho^I_{64}$</td>
<td>×</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
</tr>
</tbody>
</table>

$D_4 : fa, dup, pud, ooa, ooa$

$D_6 : pov, dov, fa, Ṋ, Ṇ$

$D_7 : □, □$
Consider an operator $\alpha$ defined over the three-valued decision set $\mathcal{D}_3 = \{1, 0, \bot\}$ defined as follows:

$$
\begin{array}{c|ccc}
\alpha & 1 & 0 & \bot \\
\hline
1 & \bot & \bot & 1 \\
0 & \bot & \bot & 0 \\
\bot & 1 & 0 & \bot \\
\end{array}
$$

1. Define $\alpha$ over the seven-valued decision set $\mathcal{D}_7$ point-wise (Recall $\mathcal{D}_7 = \wp(\mathcal{D}_3) \setminus \emptyset$)

2. Let $\mathcal{D}_6 = \{P, D, NA, I(P), I(D), I(PD)\}$ be a six-valued decision set and $\rho_{76} : \mathcal{D}_7 \rightarrow \mathcal{D}_6$ a decision reduction that maps a decision in $\mathcal{D}_7$ to a decision in $\mathcal{D}_6$ such that

$$
\rho_{76}(d) = \begin{cases} 
P & \text{if } d = 1 \\
I(P) & \text{if } d = \{1, \bot\} \\
D & \text{if } d = \{0\} \\
I(D) & \text{if } d = \{0, \bot\} \\
NA & \text{if } d = \bot \\
I(PD) & \text{if } d = \{1, 0\} \lor d = \{1, 0, \bot\} \\
\end{cases}
$$

Determine whether $\rho_{76}$ is safe with respect to the operator defined over $\mathcal{D}_7$. 
Define $\alpha$ over the seven-valued decision set $\mathcal{D}_7$ point-wise (Recall $\mathcal{D}_7 = \wp(\mathcal{D}_3) \setminus \emptyset$)

<table>
<thead>
<tr>
<th>$\alpha$</th>
<th>1</th>
<th>0</th>
<th>$\bot$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$\bot$</td>
<td>$\bot$</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>$\bot$</td>
<td>$\bot$</td>
<td>0</td>
</tr>
<tr>
<td>$\bot$</td>
<td>1</td>
<td>0</td>
<td>$\bot$</td>
</tr>
</tbody>
</table>
Define $\alpha$ over the seven-valued decision set $\mathcal{D}_7$ point-wise (Recall $\mathcal{D}_7 = \wp(\mathcal{D}_3) \setminus \emptyset$)

<table>
<thead>
<tr>
<th>$\alpha$</th>
<th>1</th>
<th>0</th>
<th>⊥</th>
<th>1, ⊥</th>
<th>0, ⊥</th>
<th>1, 0</th>
<th>1, 0, ⊥</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>⊥</td>
<td>⊥</td>
<td>1</td>
<td>1, ⊥</td>
<td>1, ⊥</td>
<td>⊥</td>
<td>1, ⊥</td>
</tr>
<tr>
<td>0</td>
<td>⊥</td>
<td>⊥</td>
<td>0</td>
<td>0, ⊥</td>
<td>0, ⊥</td>
<td>⊥</td>
<td>0, ⊥</td>
</tr>
<tr>
<td>⊥</td>
<td>1</td>
<td>0</td>
<td>⊥</td>
<td>1, ⊥</td>
<td>0, ⊥</td>
<td>1, 0</td>
<td>1, 0, ⊥</td>
</tr>
<tr>
<td>1, ⊥</td>
<td>1, ⊥</td>
<td>0, ⊥</td>
<td>1, ⊥</td>
<td>1, ⊥</td>
<td>1, 0, ⊥</td>
<td>1, 0, ⊥</td>
<td>1, 0, ⊥</td>
</tr>
<tr>
<td>0, ⊥</td>
<td>1, ⊥</td>
<td>0, ⊥</td>
<td>0, ⊥</td>
<td>1, 0, ⊥</td>
<td>0, ⊥</td>
<td>1, 0, ⊥</td>
<td>1, 0, ⊥</td>
</tr>
<tr>
<td>1, 0</td>
<td>⊥</td>
<td>⊥</td>
<td>1, 0</td>
<td>1, 0, ⊥</td>
<td>1, 0, ⊥</td>
<td>⊥</td>
<td>1, 0, ⊥</td>
</tr>
<tr>
<td>1, 0, ⊥</td>
<td>1, ⊥</td>
<td>0, ⊥</td>
<td>1, 0, ⊥</td>
<td>1, 0, ⊥</td>
<td>1, 0, ⊥</td>
<td>1, 0, ⊥</td>
<td>1, 0, ⊥</td>
</tr>
</tbody>
</table>
Safe Reduction

Solution (2)

Let $\mathcal{D}_6 = \{P, D, NA, I(P), I(D), I(PD)\}$ be a six-valued decision set and $\rho_{76} : \mathcal{D}_7 \rightarrow \mathcal{D}_6$ a decision reduction that maps a decision in $\mathcal{D}_7$ to a decision in $\mathcal{D}_6$ such that

$$\rho_{76}(d) = \begin{cases} 
P & \text{if } d = 1 \\
D & \text{if } d = \{0\} \\
NA & \text{if } d = \perp \\
I(P) & \text{if } d = \{1, \perp\} \\
I(D) & \text{if } d = \{0, \perp\} \\
I(PD) & \text{if } d = \{1, 0\} \lor d = \{1, 0, \perp\}
\end{cases}$$

Determine whether $\rho_{76}$ is safe with respect to the operator defined over $\mathcal{D}_7$.

<table>
<thead>
<tr>
<th>$\alpha$</th>
<th>1</th>
<th>0</th>
<th>$\perp$</th>
<th>1, $\perp$</th>
<th>0, $\perp$</th>
<th>1, 0</th>
<th>1, 0, $\perp$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$\perp$</td>
<td>$\perp$</td>
<td>1</td>
<td>1, $\perp$</td>
<td>1, $\perp$</td>
<td>$\perp$</td>
<td>1, $\perp$</td>
</tr>
<tr>
<td>0</td>
<td>$\perp$</td>
<td>$\perp$</td>
<td>0</td>
<td>0, $\perp$</td>
<td>0, $\perp$</td>
<td>$\perp$</td>
<td>$\perp$</td>
</tr>
<tr>
<td>$\perp$</td>
<td>1</td>
<td>0</td>
<td>$\perp$</td>
<td>1, $\perp$</td>
<td>0, $\perp$</td>
<td>$\perp$</td>
<td>1, 0</td>
</tr>
<tr>
<td>1, $\perp$</td>
<td>1, $\perp$</td>
<td>0, $\perp$</td>
<td>1, $\perp$</td>
<td>1, $\perp$</td>
<td>1, 0, $\perp$</td>
<td>1, 0, $\perp$</td>
<td>1, 0</td>
</tr>
<tr>
<td>0, $\perp$</td>
<td>1, $\perp$</td>
<td>0, $\perp$</td>
<td>0, $\perp$</td>
<td>1, 0, $\perp$</td>
<td>0, $\perp$</td>
<td>1, 0, $\perp$</td>
<td>1, 0</td>
</tr>
<tr>
<td>1, 0</td>
<td>$\perp$</td>
<td>$\perp$</td>
<td>1, 0</td>
<td>1, 0, $\perp$</td>
<td>1, 0, $\perp$</td>
<td>$\perp$</td>
<td>1, 0</td>
</tr>
<tr>
<td>1, 0, $\perp$</td>
<td>1, $\perp$</td>
<td>0, $\perp$</td>
<td>1, 0, $\perp$</td>
<td>1, 0, $\perp$</td>
<td>1, 0, $\perp$</td>
<td>$\perp$</td>
<td>1, 0</td>
</tr>
</tbody>
</table>

Observe that $\{1, 0, \perp\}$ and $\{1, 0\}$ should have the same behavior because $\rho_{76}(\{1, 0, \perp\}) = \rho_{76}(\{1, 0\})$. However:

$$\rho_{76}(\alpha(\{1\}, \{1, 0, \perp\})) = \rho_{76}(\{1, \perp\}) = I(P)$$
$$\rho_{76}(\alpha(\{1\}, \{1, 0\})) = \rho_{76}(\{\perp\}) = NA$$
Conclusion

- **Decision Reduction**
  - Deal with non-conclusive decisions
  - Reuse combining algorithms
  - Enable interoperability

- **Safe Decision Reduction**
  - Ensure that a reduction can be performed at any level of policy composition without changing the final decision

- **Safety Analysis of XACML v3**
  - XACML v3 is NOT safe!!
  - Decision set depends on combining operators
Charles Morisset, Nicola Zannone: Reduction of access control decisions. SACMAT 2014: 53-62
Exam

3 hours closed book exam

Date: 30 October 2020 13:30-16:30
Place: TBD

Exam:
▶ Exercises
  ▶ Similar to the ones given in class and homework
▶ Questions on theory
  ▶ Lectures
  ▶ Mandatory papers

Previous exams on course webpage along with solutions for some exercises