Label-Based Access Control: An ABAC Model with Enumerated Authorization Policy

Prosunjit Biswas, Ravi Sandhu and Ram Krishnan
University of Texas at San Antonio

1st Workshop on Attribute Based Access Control (ABAC 2016)
Outline

- Summary
- Background & motivation
- Enumerated authorization policy ABAC model
- Relationship with existing models
- Expressive power of LaBAC
- Conclusion
We present an enumerated authorization policy ABAC model and understand its relationship with traditional access control models.
Background and Motivation
Authorization policy

Logical formula

- Boolean expression
- E.g.: \( \text{age}(u) > 18 \)
- Models: ABAC, HGABAC

Enumeration

- Set of tuples
  - \( \{ (\text{age}(u), 19), (\text{age}(u), 20), \ldots, (\text{age}(u), 100) \} \) [assuming range upper bound \( \leq 100 \)]
- Models: Policy Machine, 2-sorted-RBAC

World-Leading Research with Real-World Impact!
Many ways to set up a policy - $\text{Auth}_{\text{read}}$
($\text{Auth}_{\text{read}}$ allows manager to read TS objects from home or office).

\[
\begin{align*}
(i) & \quad mng \in \text{role}(u) \land (\text{office} \in \text{location}(u) \lor \text{home} \in \text{location}(u)) \land \text{TS} \in \text{sensitivity}(o) \\
(ii) & \quad ((mng \in \text{role}(u) \land \text{office} \in \text{location}(u)) \lor (mng \in \text{role}(u) \land \text{home} \in \text{location}(u))) \land \text{TS} \in \text{sensitivity}(o) \\
(iii) & \quad ((mng \in \text{role}(u) \land \text{office} \in \text{location}(u) \land \text{TS} \in \text{sensitivity}(o)) \lor
\quad ((mng \in \text{role}(u) \land \text{home} \in \text{location}(u) \land \text{TS} \in \text{sensitivity}(o))
\end{align*}
\]
Update $\text{Auth}_{\text{read}}$ so that manager can no longer read $TS$ objects from home

(i) $mng \in \text{role}(u) \land (\text{office} \in \text{location}(u) \lor \text{home} \in \text{location}(u)) \land TS \in \text{sensitivity}(o)$

(ii) $((mng \in \text{role}(u) \land \text{office} \in \text{location}(u)) \lor (mng \in \text{role}(u) \land \text{home} \in \text{location}(u))) \land TS \in \text{sensitivity}(o)$

(iii) $((mng \in \text{role}(u) \land \text{office} \in \text{location}(u) \land TS \in \text{sensitivity}(o)) \lor ((mng \in \text{role}(u) \land \text{home} \in \text{location}(u) \land TS \in \text{sensitivity}(o)))$
ENUMERATED AUTH. POLICY

\[ \text{Auth}_{\text{read}} \equiv \{(\text{mng}, \text{home}, \text{TS}), (\text{mng}, \text{office}, \text{TS})\} \]

\[ \text{Auth}_{\text{read}} \equiv \{ (\text{mng, home, TS}), (\text{mng, office, TS}) \} \]
Logical formula vs enumerated policy

**Pros**

- Rich & flexible
- Easy to setup
- Concise

**Cons**

- Difficult to update
- Monolithic
- Heterogeneous

**Logical formula authorization policy**

**Enumerated authorization policy**

- Homogeneous
- Micro policy
- Easy to update

- Large in size
- Difficult to setup
LaBAC: Label-Based Access Control
Characteristics

- **Label vs Attribute**
  - Labels are attributes with tighter semantics

- **Salient features of LaBAC**
  - Finite domain ABAC
  - Simple enumerated ABAC model
Family of LaBAC models

LaBAC
(LaBAC₁)

Hierarchical LaBAC
(LaBAC₉)

Constrained LaBAC
(LaBAC₉)

Basic LaBAC
(LaBAC₀)

Figure 2: Family of LaBAC models
LaBAC: Core model

Examples

UL = \{manager, employee\}

OL = \{TS, S\}

Tuple1 = (manager, TS)

Policy_{read} = \{tuple1, tuple2\...\}

Salient Characteristics:
1. One user and object attribute
2. Atomic valued tuples
3. Tuples represent micro-policies

Figure 1

Figure 2
LaBAC: Hierarchical model

ULH={(manager, employee)}
OLH={(protected, public)}
Policy\textsubscript{a} = {(employee, protected)}
ImpliedPolicy\textsubscript{a} = {(employee, protected), (manager, protected), (employee, public), (manager, public)}

Examples

Figure 1

Figure 2
LaBAC: Constrained model

Examples

**uLabel assgn. cons:** a user cannot be both manager & director.

**Session assgn. cons:** at most one value can be activated in a session.

**oLabel assgn. cons:** A object cannot be both private & public

**Policy cons:** (employee, TS) can never be used.
Relationship of LaBAC with other enumerated policy models
LaBAC equivalent to 2-sorted-RBAC

Figure 1: 2-sorted-RBAC

Figure 2: LaBAC

2-sorted-RBAC vs LaBAC:
1. Use of attributes
2. Separation of object and action from permission
LaBAC as an instance of Policy Machine

- Policy Machine\textsubscript{\text{mini}}
  - Only ASSIGN and ASSOCIATION relation
  - Default policy class

- Configuration of LaBAC in Policy Machine\textsubscript{\text{mini}}
Flexibility in expressing traditional models
Expressiveness of LaBAC models
LBAC assumptions:
1. Tranquility
2. Object operation: creation only

\[ UL = |SC| \text{ and } |OL| = 2 \times |SC| \]
\[ |Policy| = 2 \ \text{(Policy}_{\text{read}} \text{ and Policy}_{\text{write}}) \]
Micro-policy in LaBAC
Micro-policy in LaBAC

- micro-policy as the smallest unit of administration

- Example of a micro-policy: (manager, TS)
What is next

- Any other form of representation for authorization policy?
- How expressive power of enumerated authorization policy is compared with that of logical-formula auth. policy?
- What would be the cost of storing large number of enumerated tuples?
Thank you!