Can Access Control be Extended to Deal with Data Handling in Privacy Scenarios?

Laurent Bussard and Moritz Y. Becker
Microsoft (EMIC and MSRC)

W3C Workshop on Access Control Application Scenarios
November 17th 2009
Luxembourg
Outlines

- Scenario: Privacy Policies and Preferences
- Links with Access Control
- Our work: from access control to data handling
  - SecPAL
  - SecPAL for Privacy
- Relevance for XACML
- Questions and Discussion
General Scenario

1) Policy

User (data subject)

2) Pref.

3) Can I share? (Matching)

4) PII + SP

Service (data controller)

5) store

6) Can I use for... ?

7) Obligations

8) Can I share?

Third Party (downstream data controller)

PII + SP'
State of the art: APPEL, P3P, EPAL
state of the art: PRIME

PRIME-DHP

PRIME-obligations

PRIME-AC

User (data subject)

Service (data controller)

Third Party (downstream data controller)

2) Pref.

3) Can I share? (Matching)

4) PII + SP

5) store

6) Can I use for...?

7) Obligations

8) Can I share? 

PII + SP'
Shortcoming of state of the art
Access Control vs. Data Handling

**Access Control (AC)**

- Service (S)
  - Data (D_S), AC-Policy
- Client (C)
  - Credentials (C_C)

1) Get D_S, C_C

2) Query: can I share Data with C according to AC-Policy and C_C?

2') Obligation triggered by AC decision

3) D_S

4) Use D_S

**Data Handling (DH)**

- Data Subject (S)
  - (user)
  - Data (D_S), DH-Pref
- Data Controller (C)
  - (service)
  - Cred. (C_C), DH-Policy

1) Get D_S, C_C, DH-Policy

2) Query: can I share D_S with C according to DH-Pref, DH-Policy, and C_C?

3) D_S (Sticky Policy)

4) Query: can I use D_S for purpose P?

5) Query: can I share D_S with C’?

6) Obligation triggered by event.

**Main differences:**

- In DH, “AC” query (2) takes two “policies” into account.
- In DH, two parties specify (Sticky) Policy of C (including obligations)
- In DH, C has to evaluate “AC” queries.
- In DH, obligations are not only triggered by AC decisions
SecPAL (in one slide)

- AC Policy (assertions)
  - Service says CA can say \( x \) is a researcher (A1)
  - Service says \( y \) can read /project/data if \( y \) is a researcher (A2)

- Credentials (assertions)
  - CA says Bob is a researcher (A3)

- AuthZ Query:
  - Service says Bob can read /project/data/file\( _1 \)? (Q1)
    Q1 succeeds because \( A_1 + A_3 \) → Service says Bob is a researcher
    and because \( A_2 + (A_1 + A_3) \) → Service says Bob can read /project/data

- Key features:
  - Balance between simplicity and expressiveness
  - Syntax close to natural language
  - Semantics consists of just three deduction rules
  - Logic-based: translation to “Datalog with Constraints”
SecPAL for Privacy

- User’s Preference
  - Rights
    \(<\text{Usr}>\) says \(<\text{Svc}>\) may use Email for \(p\) where \(p \in \{\text{Confirm}; \text{Marketing}; \text{Stats}\}\)
  - Obligations
    \(\exists t\) (<Svc> says <Svc> will delete Email within \(t \leq 2\) yr) ?
  - \(\text{(MA1)}\)

- Service’s Policy
  - Rights
    \(<\text{Usr}>\) says \(<\text{Svc}>\) may use Email for Marketing ?
  - Obligations
    \(<\text{Svc}>\) says \(<\text{Svc}>\) will delete Email within 1 yr
  - \(\text{(MQ1)}\)
  - \(\text{(WA1)}\)

- Data is shared if WQ1 and MQ1 succeed.

- This is not a complete example
  - Oversimplified policy and preference
  - Only shows matching (other queries at service)
  - Multi-hops data sharing and delegation are not presented here
Example: SecPAL for Privacy

Alice

E-mail address

E-mail address

eBooking

eMarketing

Alice’s preference

Pr.1 Alice says \( x \) may use Email for \( p \) if
\( x \) is a BookingSvc, where \( p \in \{ \text{Confirmation, Newsletter, Stats} \} \)

Pr.2 Alice says \( x \) may delete Email within \( t \)

Pr.3 Alice says \( x \) can send Email to \( y \) if
\( x \) is a BookingSvc,
\( y \) is a TrustedPartner

Pr.4 Alice says CA can say \( x \) is a \( y \)

Pr.5 Alice says \( x \) can say \( y \) is a TrustedPartner if
\( x \) is a BookingSvc

PrQ.6 Alice says \( (\text{Svc}) \) is a RegisteredSvc? \( \land \)
\( \exists t \) \((\text{Svc}) \) says \( (\text{Svc}) \) will delete Email within \( t \)? \( \land \) \( t \leq 30 \) days?)

eBooking’s policy

Pl.1 eBooking says eBooking will delete Email within 15 days

Pl.2 CA says eBooking is a RegisteredSvc

Pl.3 CA says eBooking is a BookingSvc

PlQ.4 \((\text{Usr})\) says eBooking may use Email for Confirmation? \( \land \)
\((\text{Usr})\) says eBooking may use Email for Stats? \( \land \)
\((\text{Usr})\) says eBooking may delete Email within 15 days? \( \land \)
\((\text{Usr})\) says eBooking may send Email to eMarketing?

eBooking says eMarketing is a TrustedPartner

eMarketing’s preferences

Pl’.1 eMarketing says eMarketing will delete Email within 30 days

Pl’.2 CA says eMarketing is a RegisteredSvc

PlQ’.3 \((\text{Usr})\) says eMarketing may use Email for Marketing? \( \land \)
\((\text{Usr})\) says eMarketing may delete Email within 30 days?
**XACML as DH-aware AC?**

<table>
<thead>
<tr>
<th>Requirements</th>
<th>SecPAL for Privacy</th>
<th>DH-aware XACML</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specification of access control rules</td>
<td>may-assertions</td>
<td>XACML policy (+ extensions)</td>
</tr>
<tr>
<td>Authorization queries</td>
<td>may-queries</td>
<td>XACML query (input to PDP)</td>
</tr>
<tr>
<td>Specification of generic obligations</td>
<td>will-assertions</td>
<td>XACML-obligation (+ extensions)</td>
</tr>
<tr>
<td>Obligation queries</td>
<td>will-queries</td>
<td>-</td>
</tr>
<tr>
<td>Specification of attributes and rights</td>
<td>usual SecPAL assertions</td>
<td>SAML assertions</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Actors</th>
<th>SecPAL for Privacy</th>
<th>DH-aware XACML</th>
</tr>
</thead>
<tbody>
<tr>
<td>User agent</td>
<td>SecPAL engine</td>
<td>XACML PDP</td>
</tr>
</tbody>
</table>
Expressing the upper bound on behaviors (may verb) should be possible with XACML.

- Data subject's preferences: a XACML policy
- Data controller's preferences would be a set of queries.

The user agent = Policy Decision Point.

Extensions required:
- handle “purpose”
- placeholders that are instantiated before evaluating the query.
Lower bound (will) in XACML

- **Data controller's side:**
  - complete specification of XACML obligations
  - support for obligations that are not triggered by access control decision.
  - Part of this may be covered by ongoing work on a proposal for obligations in XACML 3.0.

- **Data subject’s side:**
  - a language to query obligations would be necessary.

- Lower and upper bound should be comparable.
Questions and Discussion

- Should we consider XACML in such scenarios?
- Are lessons learned from extending SecPAL towards data handling applicable to XACML?
- Should XACML obligations support other types of triggers?
- How to serialize “XACML queries”?
- How to specify “obligation queries”?
- Multiple languages (upper and lower)?

Contact: LBussard@microsoft.com
Details on SecPAL (for Privacy): http://research.microsoft.com/SecPAL
SecPAL for Privacy: User’s Preferences

Pr.1  Alice says $x$ may use Email for $p$ if
       $x$ is a BookingSvc,
       where $p \in \{\text{Confirmation, Newsletter, Stats}\}$

Pr.2  Alice says $x$ may delete Email within $t$

Pr.3  Alice says $x$ may send Email to $y$ if
       $x$ is a BookingSvc,
       $y$ is a TrustedPartner

Pr.4  Alice says CA can say $x$ is a $y$

Pr.5  Alice says $x$ can say $y$ is a TrustedPartner if
       $x$ is a BookingSvc

PrQ.6  Alice says $\langle Svc \rangle$ is a RegisteredSvc? \&
        \exists t (\langle Svc \rangle$ says $\langle Svc \rangle$ will delete Email within $t$? \& $t \leq 30$ days?)
SecPAL for Privacy: Services’ Policy

P1.1  
eBooking says eBooking will delete Email within 15 days

P1.2  
CA says eBooking is a RegisteredSvc

P1.3  
CA says eBooking is a BookingSvc

P1Q.4  
⟨Usr⟩ says eBooking may use Email for Confirmation?  ∧
⟨Usr⟩ says eBooking may use Email for Stats?  ∧
⟨Usr⟩ says eBooking may delete Email within 15 days?  ∧
⟨Usr⟩ says eBooking may send Email to eMarketing?

eBooking says eMarketing is a TrustedPartner

P1’.1  
eMarketing says eMarketing will delete Email within 30 days

P1’.2  
CA says eMarketing is a RegisteredSvc

P1Q’.3  
⟨Usr⟩ says eMarketing may use Email for Marketing?  ∧
⟨Usr⟩ says eMarketing may delete Email within 30 days?