Attribute Based Access Control

Example
### StreamingMoviesRUs.com

<table>
<thead>
<tr>
<th>Movie Rating</th>
<th>Users Allowed Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>R</td>
<td>Age 17 and older</td>
</tr>
<tr>
<td>PG-13</td>
<td>Age 13 and older</td>
</tr>
<tr>
<td>G</td>
<td>Everyone</td>
</tr>
</tbody>
</table>

The website must enforce this access control policy
RBAC method

• Every user is assigned one of three roles when they register for the web site:
  – Adult
  – Juvenile
  – Child

• Permissions:
  – can view R-rated movies
  – can view PG13 movies
  – can view G-rated movies

• User to role and Permission to role assignments are an administrative task
  – Example, ADULT role gets all 3 permissions
ABAC implementation

• No need to create roles
• Attributes
  – User: age
  – Movie: rating
• Policy:
  – Rule: can_access(u,m,e) =
    • Age(u) >=17 and rating in {R,PG13,G} OR
    • Age(u) >=13 AND age(u) <17 AND rating in {PG13,G} OR
    • Age(u) < 13 AND rating in {G}
ABAC flexibility for granularity

• Add more attributes
  – User is premium member or normal member
  – Movie is new-release vs old

• Enforce a rule that only premium members can view new movies.
  – RBAC: have to double the roles to distinguish by age and fee paid. Have to double permissions as well
  – ABAC: just add 2 rules