
Tanjila Mawla
Department of Computer Science
Tennessee Tech University

Maanak Gupta
Department of Computer Science
Tennessee Tech University

Ravi Sandhu
Institute for Cyber Security (ICS) and NSF C-SPECC Center,
University of Texas at San Antonio

ACM Symposium on Access Control Models and Technologies
June 8 - 10th, 2022
Activity - Centric Access Control

- The notion of Activity
- Authorization (A)
- Obligations (B)
- Conditions (C)
- Dependencies among Activities (D)
Table 1: Comparison Overview of Features Proposed in ACAC Model with other related models.

<table>
<thead>
<tr>
<th>Models</th>
<th>Notion of Activity</th>
<th>Multiple Object Activities</th>
<th>Activities Concurrency</th>
<th>Activity Precedence</th>
<th>Activities Dependency</th>
<th>Incompatible Activities</th>
<th>Conditional Constraints</th>
<th>Activities Mutability</th>
<th>Run-time Authorization</th>
<th>Obligations</th>
</tr>
</thead>
<tbody>
<tr>
<td>TBAC</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>UCON</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>ACON</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>ABAC</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>ACAC</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
</tbody>
</table>
Figure 1: ACAC Model Components.
Figure 2: A Framework for a Hierarchy of ACAC models
Figure 3: States of an Activity
Table 2: Mutability of Dependent Activities in terms of the invocation time related to a requested activity. √ and × respectively denote the presence (mandatory or optional) and absence of the corresponding field to support the relationships in the first column

<table>
<thead>
<tr>
<th>Activities Relationship</th>
<th>Immutable</th>
<th>Pre-invocation</th>
<th>Parallel invocation</th>
<th>Post-invocation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Independent</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Ordered</td>
<td>×</td>
<td>√</td>
<td>×</td>
<td>√</td>
</tr>
<tr>
<td>Concurrent</td>
<td>×</td>
<td>×</td>
<td>√</td>
<td>×</td>
</tr>
<tr>
<td>Temporary</td>
<td>×</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Precedence</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>√</td>
</tr>
<tr>
<td>Conditional</td>
<td>×</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Incompatible</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
</tr>
</tbody>
</table>
ACAC and Zero-Trust

- All data sources and computing services are considered resources.
- All communication is secured regardless of network location.
- Access to individual enterprise resources is granted on a per-session basis.
- Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.
- The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.
Future Research Agenda

• Operational and administrative formal model.
• Policy language and enforcement architecture.
• Risk adaptive ACAC incorporating zero-trust tenets.
• Self-adaptive and AI-driven ACAC Deployment
Selected References


Thank You!

Questions?