Role-Based Access Control Modelling

1. How is a specific type of interaction between a subject and an object that results in the flow of information from one to another called?

☐ Access control
☐ Session
☐ Access
☐ Permission assignment
RBAC: Role-based Access Control

Access – a specific type of interaction between a subject and an object that results in the flow of information from one to the other

Access control – the process of limiting access to the resources of a system only to authorised programs, processes or other systems
Role-Based Access Control Modelling

1. How is a specific type of interaction between a subject and an object that results in the flow of information from one to another called?

☐ Access control
☐ Session
☒ Access
☐ Permission assignment
Role-Based Access Control Modelling

2. How is an active entity that causes information to flow among objects or changes the system state called?

☐ Administrator
☐ User
☐ Subject
☐ Role
Subject - an active entity that causes information to flow among objects or changes the system state

Sandhu and Coyne, 1996; Ferraiolo et al., 2001
Role-Based Access Control Modelling

2. How is an active entity that causes information to flow among objects or changes the system state called?

☐ Administrator
☐ User
☑ Subject
☐ Role
Role-Based Access Control Modelling

3. How is a partial order of relationships established among roles called?

☐ Sessions
☐ Permission hierarchy
☐ Role hierarchy
☐ Constraints
RBAC family

- **RBAC\(_0\)**
  - Everything except role hierarchies and constraints

- **RBAC\(_1\)**
  - RBAC\(_0\) plus role hierarchies

- **RBAC\(_2\)**
  - RBAC\(_0\) plus role constraints

- **RBAC\(_3\)**
  - RBAC\(_1\) plus RBAC\(_2\)

---

Role hierarchy — a partial order relationship established among roles

Constraint — a relationship among roles

Sandhu and Coyne, 1996; Ferraiolo et al., 2001
Role-Based Access Control Modelling

3. How is a partial order of relationships established among roles called?

☐ Sessions
☐ Permission hierarchy
☒ Role hierarchy
☐ Constraints
Role-Based Access Control Modelling

4. What are the major tasks of the system administrator?

☐ Predefine secured operations and objects
☐ Manage users and roles
☐ Create assignment relationships
☐ Establish relationships between roles, secured operations and objects
Implementation requirements

**System administrator** – the individual who establishes the system security policies, performs the administrative roles and reviews the system audit trail.

- **Operations** and **Objects** are considered predefined by the underlying system.

- **Administrator**
  - manage **Users, Roles**
  - create assignment relationships
  - establish relationships between **Roles** and secured **Operations** and **Objects**.

Sandhu and Coyne, 1996; Ferraiolo et al., 2001
Role-Based Access Control Modelling

4. What are the major tasks of the system administrator?

- Predefine secured operations and objects
- Manage users and roles
- Create assignment relationships
- Establish relationships between roles, secured operations and objects
Role-Based Access Control Modelling

5. Which modelling languages are specifically extended to model role-based access control?

☐ Secure Tropos
☐ SecureUML
☐ KAOS extension to security
☐ Misuse cases
☐ Mal-activity diagrams
☐ UMLsec
Security Modelling Languages

<table>
<thead>
<tr>
<th>Early requirements</th>
<th>Late requirements</th>
<th>Architectural design</th>
<th>Detailed design</th>
<th>Implementation and testing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure TROPOS</td>
<td>KAOS extension to security</td>
<td>Misuse cases</td>
<td>Mal-activity diagrams</td>
<td>SecureUML</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>UMLsec</td>
</tr>
</tbody>
</table>
Role-Based Access Control Modelling

5. Which modelling languages are specifically extended to model role-based access control?

☐ Secure Tropos
☒ SecureUML
☐ KAOS extension to security
☐ Misuse cases
☐ Mal-activity diagrams
☒ UMLsec
Role-Based Access Control Modelling

6. What are the main security actions?

☐ Insert / create
☐ Select / read
☐ Change / update
☐ Remove / delete
Access Rules

- Security actions
Role-Based Access Control Modelling

6. What are the main security actions?

- Insert / create
- Select / read
- Change / update
- Remove / delete
7. There exist different access control models besides the role-based access control (RBAC) model. Please write names of at least 2 other access control models
Further reading

Access Control Approaches

• **ABAC:** Attribute-based access control  
  [Hu et al., 2014, 2015]

• **UCON:** Usage control model  
  [Park and Sandhu, 2004]

• **RAdAC:** Risk-adaptive access control  
  [McGraw, 2009; Shaikh et al., 2012]

• **TBAC:** Token-based access control  
  [Radhakrishnan, 2012]
There exist different access control models besides the role-based access control (RBAC) model. Please write names of at least 2 other access control models.

- **ABAC**: Attribute-based access control
- **UCON**: Usage control model
- **RAdAC**: Risk-adaptive access control
- **TBAC**: Token-based access control