Test 3 - Feedback

Lectures
6. Security Modelling: Designing secure system functions and behavior
7. Privacy Modelling
10. Role-based access control

Asset-related concepts

<table>
<thead>
<tr>
<th>ISSRM concept</th>
<th>Constructs or their combination</th>
<th>Concrete syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset</td>
<td>C Actor</td>
<td><img src="image" alt="Actor" /></td>
</tr>
<tr>
<td>System asset</td>
<td>C (IS) use case System boundary</td>
<td><img src="image" alt="System boundary" /></td>
</tr>
<tr>
<td>Business asset</td>
<td>C (Business) use case</td>
<td><img src="image" alt="Use case" /></td>
</tr>
<tr>
<td>Security criterion</td>
<td>C Security criterion</td>
<td><img src="image" alt="Security criterion" /></td>
</tr>
<tr>
<td>constraint of</td>
<td>R constraint of</td>
<td><img src="image" alt="constraint of" /></td>
</tr>
</tbody>
</table>

Modelling languages

1. Which of the following constructs can be used to represent system assets in Security risk-oriented misuse cases?

   - [ ] Security Use Case
   - [x] System Boundary
   - [x] Use Case
Modelling languages

2. Which of the following constructs can be used to represent vulnerability in Security risk-oriented misuse cases?

☐ Misuser
☐ Misuse case
☒ Vulnerability

3. Which of the following constructs can be used to represent impact using Mal-activities for the risk management?

☐ Swimlane
☐ Decisions
☐ Malicious Activity
3. Which of the following constructs can be used to represent impact using Mal-activities for the risk management?

☐ Swimlane
☐ Decisions
☒ Malicious Activity

4. Which of the following constructs can be used to represent control using Mal-activities for the risk management?

☐ Mitigation Activity
☐ Swimlane
☐ Activity
☐ Decision

Risk-related concepts

<table>
<thead>
<tr>
<th>ISSRM concept</th>
<th>Mal-activity diagram</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk</td>
<td>Combination of constructs representing Event and Impact</td>
</tr>
<tr>
<td>Impact</td>
<td>Mal-activity</td>
</tr>
<tr>
<td>Event</td>
<td>Combination of constructs representing Threat and Vulnerability</td>
</tr>
<tr>
<td>Vulnerability</td>
<td>As informal comment linked to vulnerable system assets</td>
</tr>
<tr>
<td>Threat</td>
<td>Combination of constructs representing Threat agent and Attack method</td>
</tr>
<tr>
<td>Threat agent</td>
<td>Mal-activity</td>
</tr>
</tbody>
</table>
| Attack method | a) Process described using Mal-activity, Mal-decision, and ControlFlows
                b) Swimlane (as means to perform the attack) |
|               | uses
|               | targets, harms, leads to exploits, negates |

Modelling languages
Modelling languages

4. Which of the following constructs can be used to represent control using Mal-activities for the risk management?

☐ Mitigation Activity
☒ Swimlane
☐ Activity
☐ Decision

Model transformation

How to transform security risk management model from Security risk-oriented misuse cases (misuse cases) to Mal-activities for the risk management (mal-activity)?

5. Regarding system asset

☐ From misuse cases Security Constraint to mal-activity Activity
☐ From misuse cases Use case to mal-activity Activity
☒ From misuse cases Use case to mal-activity Comment

TR.MUC-MAL.3: A use case construct is translated to the activity construct.
Model transformation

6. Regarding attack method

☐ From misuse cases Misuse case to mal-activity Mitigation activity
☐ From misuse cases Misuse case to mal-activity Malicious activity
☐ From misuse cases Misuser to mal-activity Mal-swimlane

Model transformation

How to transform security risk management model from Security risk-oriented misuse cases (misuse cases) to Mal-activities for the risk management (mal-activity)?

Privacy properties

7. What does it mean when an attacker cannot sufficiently distinguish whether an item of interest (from the attacker’s perspective) exists or not?

☐ Unlinkability
☐ Undetectability
☐ Unobservability
7. What does it mean when an attacker cannot sufficiently distinguish whether an item of interest (from the attacker’s perspective) exists or not?

- Undetectability
- Unobservability

8. What does it mean when an attacker cannot sufficiently identify the subject within a set of subjects (from the attacker perspective)?

- Anonymity
- Unobservability
- Pseudonymity
Privacy properties

8. What does it mean when an attacker cannot sufficiently identify the subject within a set of subjects (from the attacker perspective)?

- [x] Anonymity
- [ ] Unobservability
- [ ] Pseudonymity

Privacy properties

9. What does it mean “PET” in the context of the privacy-by-design?

- [ ] A domestic or tamed animal kept for companionship or pleasure
- [x] Privacy enhancing technology
- [ ] Privacy enforcing technique
- [ ] Policy enhancing technology
Role-Based Access Control Modelling

10. 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

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

☐ Administrator
☐ User
☐ Subject
☐ Role

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

- Administrator
- User
- **Subject**
- Role

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

- Sessions
- Permission hierarchy
- **Role hierarchy**
- Constraints

---

**Role-Based Access Control Modelling**

**RBAC**

- **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

---

*Sandhu and Coyne, 1996; Ferraiolo et al., 2001*
12. How is a partial order of relationships established among roles called?

- ☐ Sessions
- ☐ Permission hierarchy
- ✗ Role hierarchy
- ☐ Constraints

13. 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

- 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
14. 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

15. What are the main security actions?

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

• Security actions

Exercise 1: In the given Mal-activities for security risk management model (see Fig. 1), identify which elements represent:

• Impact:

• Attack method:

• Security requirements:
Exercise 1: In the given Mal-activities for security risk management model (see Fig. 1), identify which elements represent:

- **Impact:**
  - Modify game report
  - Pass game report

- **Attack method:**
  - Intercept transfer of game report
  - Intercepted channel

- **Security requirements:**
  - Use secure communication
  - Make game report not readable (check if Changeable)

Exercise 2: Fill in the **Visibility matrix** (Table 1) with values V (visible), A (accessible), and H (hidden) for the model given in Fig. 2.

---

**Generic Stereotypes Modelling**

**Information Disclosure Analysis**

- **Visibility matrix** – overview of the data objects that each actor possesses at some point along the process
  - Visible (V) – object is owned or obtained at some point by an actor and is fully readable
  - Accessible (A) – object is owned or obtained by an actor at some point, but it is protected
  - Hidden (H) – object is owned or obtained by an actor at some point but its contents are unreadable

---

<table>
<thead>
<tr>
<th>Data-objects</th>
<th>D1</th>
<th>D2</th>
<th>D3</th>
<th>D4</th>
<th>D5</th>
<th>D6</th>
<th>D7</th>
<th>D8</th>
<th>D9</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rapid GIS App</td>
<td>V</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PE Android</td>
<td></td>
<td>V</td>
<td>H</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compute Server</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>V</td>
<td>H</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operator</td>
<td>V</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D2.1</td>
<td>D2.2</td>
<td>D4.1</td>
<td>D4.2</td>
<td>D5.1</td>
<td>D5.2</td>
<td>D6.1</td>
<td>D6.2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Exercise 2: Fill in the Visibility matrix (Table 1) with values \( V \) (visible), \( A \) (accessible), and \( H \) (hidden) for the model given in Fig. 2.

<table>
<thead>
<tr>
<th></th>
<th>D1</th>
<th>D2.1</th>
<th>D2.2</th>
<th>D4.1</th>
<th>D4.2</th>
<th>D5.1</th>
<th>D5.2</th>
<th>D6.1</th>
<th>D6.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>RapidGetterApp</td>
<td>V</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PE Android</td>
<td>V</td>
<td>A</td>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compute Server 1</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compute Server 2</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Exercise 3: The SecureUML model (see Fig. 3) was received by transforming the corresponding UMLsec model. Complete this SecureUML model by introducing missing language constructs. Do not forget (!) to define and apply needed security actions.

SecureUML model

Finish the transformation manually

- Attributes of the «umlssec.resource» class that define the state of the secured resource(s)
- Names for the association classes
- Multiplicities for all the association relationships
- Necessary authorisation constraints

SecureUML model
Authorisation Constraints

AC#1:

context Game::createGame(): void
pre: self.responsibleFFE.assignedUser -> exists(i | i.assignedUser = 'Bob')

AC#2:

context Game::updateConfirmation(): void
pre: self.responsibleFFE.assignedUser -> exists(i | i.assignedUser = 'Bob')

Exercise 4: 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]
Exercise 4: 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