Chapter 8: Mal-activities for Security Risk Management

Raimundas Matulevičius

University of Tartu, Estonia, rma@ut.ee

Goal

• Understand how security risks can be captured at the functional definition of the software system
• Explain how mal-activities are used to manage security risk
Outline

• Activities and Mal-activities
• Security risk management
  – Abstract and concrete syntax
  – Semantics
• Example
• Further reading
Activity and Mal-activity diagrams

- **Activity diagrams**
  - Represent dynamic behaviour
  - stepwise activities and actions with support for choice, iteration and concurrency
  - intended for computational and organisational processes

![Diagram of activity and mal-activity diagrams]

© Springer International Publishing AG 2017
Activity and Mal-activity diagrams

• **Activity diagrams**
  – Represent dynamic behaviour
  – stepwise activities and actions with support for choice, iteration and concurrency
  – intended for computational and organisational processes

• **Mal-activity diagrams**
  – Derived by extending activity diagrams
  – Deal with behavioural aspects of security problems
  – Define the malicious – unwanted – behaviour
Outline

- Activities and Mal-activities
- Security risk management
  - Abstract and concrete syntax
    - Semantics
- Example
- Further reading
Abstract and Concrete syntax

Concepts

© Springer International Publishing AG 2017
Abstract and Concrete syntax

Relationships

Diagram showing relationships between elements such as Initial State, Final State, Mitigation Link, Control Flow, Any Activity, Any Decision, Vulnerability, Security Criterion, Mitigation Activity, Mal-activity, and Activity.
Abstract and Concrete syntax

Relationships

Outline

• Activities and Mal-activities
• Security risk management
  – Abstract and concrete syntax
    – Semantics
• Example
• Further reading
## Asset-related concepts

<table>
<thead>
<tr>
<th>ISSRM concept</th>
<th>Mal-activity diagrams</th>
<th>Concrete syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset</td>
<td>Process described using <em>Activity, Decision,</em> and <em>ControlFlow</em> constructs</td>
<td></td>
</tr>
<tr>
<td>Business asset</td>
<td>(implicit) Objects used to perform activities</td>
<td></td>
</tr>
<tr>
<td>System asset</td>
<td><em>Swimlane</em></td>
<td></td>
</tr>
<tr>
<td>supports</td>
<td><em>ControlFlow,</em> (Implicit) <em>Swimlane</em> contains <em>FlowObjects</em> (representing Business assets)</td>
<td></td>
</tr>
<tr>
<td>Security criterion</td>
<td>As informal comment linked to business asset</td>
<td></td>
</tr>
</tbody>
</table>

## Risk-related concepts

<table>
<thead>
<tr>
<th>ISSRM concept</th>
<th>Mal-activity diagram</th>
<th>Concrete syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk</td>
<td>Combination of constructs representing <em>Event</em> and <em>Impact</em></td>
<td></td>
</tr>
<tr>
<td>Impact</td>
<td>Pass through the process represented by the <em>Mal-activity</em></td>
<td></td>
</tr>
<tr>
<td>Event</td>
<td>Combination of constructs representing <em>Threat</em> and <em>Vulnerability</em></td>
<td></td>
</tr>
<tr>
<td>Vulnerability characteristic of</td>
<td>As informal comment linked to vulnerable system assets</td>
<td></td>
</tr>
<tr>
<td>Threat</td>
<td>Combination of constructs representing Threat agent and Attack method</td>
<td></td>
</tr>
<tr>
<td>Threat agent</td>
<td><em>Mal-swimlane</em></td>
<td></td>
</tr>
<tr>
<td>Attack method</td>
<td>a) Process described using <em>Mal-activity, Mal-decision,</em> and <em>ControlFlow</em></td>
<td></td>
</tr>
<tr>
<td></td>
<td>b) <em>Swimlane</em> (as means to perform the attack)</td>
<td></td>
</tr>
<tr>
<td>uses</td>
<td>(implicit) <em>Swimlane</em> contains <em>FlowObjects</em> (representing Attack method)</td>
<td></td>
</tr>
<tr>
<td>targets, harms, leads to exploits, negates</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Risk treatment-related concepts

<table>
<thead>
<tr>
<th>ISSRM concept</th>
<th>Mal-activity diagrams</th>
<th>Constructs or their combination</th>
<th>Concrete syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk treatment</td>
<td></td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Security requirement</td>
<td>MitigationActivity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control</td>
<td>Swimlane</td>
<td></td>
<td></td>
</tr>
<tr>
<td>refines</td>
<td></td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>mitigate</td>
<td>MitigationLink</td>
<td></td>
<td></td>
</tr>
<tr>
<td>implements</td>
<td>(implicit) FlowObjects (representing security requirements) are contained in the Swimlane</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Outline

- Activities and Mal-activities
- Security risk management
  - Abstract and concrete syntax
  - Semantics
- Example
- Further reading
1. Context and assets identification
2. Security objectives determination

- Description of organisation and its environment
  - sensitive activities related to information security
3. Risk analysis

4. Risk treatment decisions

<table>
<thead>
<tr>
<th>Risk treatment decisions</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avoiding risk</td>
<td>Decision not to be involved in, or to withdraw from a risk</td>
</tr>
<tr>
<td>Transferring risk</td>
<td>Sharing with another party the burden of loss for a risk</td>
</tr>
<tr>
<td>Retaining risk</td>
<td>Accepting the burden of loss from a risk</td>
</tr>
<tr>
<td>Reducing risk</td>
<td>Action to lessen the probability, negative consequences, or both, associated with a risk</td>
</tr>
</tbody>
</table>
5. Security requirements definition
6. Control selection and implementation

6. Control selection and implementation
Outline

• Activities and Mal-activities
• Security risk management
  – Abstract and concrete syntax
  – Semantics
• Example

Further reading

• Misuse case maps [Karpati et al., 2010]
• Elicitation of security requirements through misuse case activities [Braz et al., 2008]
• Extensions of activity diagrams to specify security requirements in business processes [Rodriguez et al., 2011]
  – Notations for security requirements:
    • audit registration, access control attack harm detection, integrity, nonrepudiation and privacy requirements
Summary

- Activities and Mal-activities
- Security risk management
  - Abstract and concrete syntax
  - Semantics
- Example
- Further reading