Chapter 7: Security Risk-Oriented Misuse Cases

Raimundas Matulevičius
University of Tartu, Estonia, rma@ut.ee

Goal

• Understand how security risks can be captured and managed at the system functionality
• Explain how use case and misuse cases are aligned to the security risk management
Outline

• Use and misuse cases
• Security risk management
  – Abstract and concrete syntax
  – Semantics
• Example
• Further reading
Use Cases

• **What functions will the new system provide?**
  – How will people interact with it?
  – Describe functions from a user’s perspective

• **Use Cases**
  – Used to show:
    • the **functions** to be provided by the system
    • which **actors** will use which functions
  – Each Use Case is:
    • a pattern of behavior that the new system is required to exhibit
    • a sequence of related actions performed by an actor and the system via a dialogue

• **An actor**
  – anything that needs to interact with the system/software:
    • a person
    • a role that different people may play
    • another (external) system/software
Misuse cases

• **A modeling technique – misuse cases**
  – Normal actors and wanted functionality +
  – Mis-users, harmful acts

• **Makes it possible to discuss**
  – Security requirements together with functional requirements.
  – With a technique that is
    • In normal use
    • Relatively easy to understand for end-users

• **As with use-cases, there are two possibilities**
  – Diagrams
  – Textual descriptions
Abstract and Concrete syntax

[Diagram of abstract and concrete syntax with class relationships and associations]

Abstract and Concrete syntax

[Diagram of abstract and concrete syntax with class relationships and associations]
Abstract and Concrete syntax
Abstract and Concrete syntax

[Diagram of abstract and concrete syntax with UML class diagrams and association rules.]

© Springer International Publishing AG 2017
Outline

• Use and misuse cases
• Security risk management
  – Abstract and concrete syntax
  – Semantics
• Example
• Further reading

Asset-related concepts

<table>
<thead>
<tr>
<th>ISSRM concept</th>
<th>Misuse cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset</td>
<td>C Actor</td>
</tr>
<tr>
<td>System asset</td>
<td>C (IS) use case System boundary</td>
</tr>
<tr>
<td>Business asset</td>
<td>C (Business) use case</td>
</tr>
<tr>
<td>supports</td>
<td>R Explicitly: includes and extends</td>
</tr>
<tr>
<td></td>
<td>Implicitly: business asset constructs that are under the system boundary</td>
</tr>
<tr>
<td>Security criterion</td>
<td>C Security criterion</td>
</tr>
<tr>
<td>constraint of</td>
<td>R constraint of</td>
</tr>
</tbody>
</table>
### Risk-related concepts

<table>
<thead>
<tr>
<th>ISSRM concept</th>
<th>Misuse cases</th>
<th>Constructs or their combination</th>
<th>Concrete syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk</td>
<td>C</td>
<td>A combination of constructs used to express event and impact</td>
<td>![Diagram]</td>
</tr>
<tr>
<td>Impact</td>
<td>C</td>
<td>Impacts (stereotype)</td>
<td>![Diagram]</td>
</tr>
<tr>
<td>Event</td>
<td>C</td>
<td>A combination of constructs used to express threat and vulnerability</td>
<td>![Diagram]</td>
</tr>
<tr>
<td>Attack method</td>
<td>C</td>
<td>Misuse cases</td>
<td>![Diagram]</td>
</tr>
<tr>
<td>Vulnerability</td>
<td>C</td>
<td>Vulnerability (stereotype)</td>
<td>![Diagram]</td>
</tr>
<tr>
<td>Threat agent</td>
<td>C</td>
<td>Misuser</td>
<td>![Diagram]</td>
</tr>
<tr>
<td>Threat</td>
<td>C</td>
<td>A combination of misuser and misuse case using communication link</td>
<td>![Diagram]</td>
</tr>
</tbody>
</table>

**Target Links**
- `targets`: `threaten link`  
- `exploits`: `exploit link`  
- `negates`: `negate link`  
- `harms`: `harm link`  
- `lead to`: `lead to link`  
- `characteristic of`: `include links`  
- `uses`: `communication link`

### Risk treatment-related concepts

<table>
<thead>
<tr>
<th>ISSRM concept</th>
<th>Misuse cases</th>
<th>Constructs or their combination</th>
<th>Concrete syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk treatment</td>
<td>C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security requirement</td>
<td>C</td>
<td>(Security) use case</td>
<td>![Diagram]</td>
</tr>
<tr>
<td>Control</td>
<td>C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>refines</td>
<td>R</td>
<td></td>
<td></td>
</tr>
<tr>
<td>mitigate</td>
<td>R</td>
<td>mitigate link</td>
<td></td>
</tr>
<tr>
<td>implements</td>
<td>R</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Outline

• Use and misuse cases
• Security risk management
  – Abstract and concrete syntax
  – Semantics
• Example
• Further reading

Security risk management process
1. Context and assets identification

2. Security objectives determination
   - Description of organisation and its environment
     - sensitive activities related to information security

3. Risk analysis
3. Risk analysis

<table>
<thead>
<tr>
<th>Name</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Basic path</strong></td>
<td>actions that the misuser(s) and the system go through to harm the proposed system</td>
</tr>
<tr>
<td><strong>Mitigation points</strong></td>
<td>actions in a basic or alternative path where misuse can be mitigated</td>
</tr>
<tr>
<td><strong>Trigger</strong></td>
<td>states or events in the system or its environment that may initiate the misuse case</td>
</tr>
<tr>
<td><strong>Assumption</strong></td>
<td>states in the system’s environment that make the misuse case possible</td>
</tr>
<tr>
<td><strong>Precondition</strong></td>
<td>system states that make the misuse case possible</td>
</tr>
<tr>
<td><strong>Mitigation point</strong></td>
<td>guaranteed outcome of mitigating a misuse case</td>
</tr>
<tr>
<td><strong>Stakeholder and risks</strong></td>
<td>major risks for each stakeholder involved in the misuse case</td>
</tr>
</tbody>
</table>

![Diagram of Risk Analysis Process](image-url)
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
Outline

• Use and misuse cases
• Security risk management
  – Abstract and concrete syntax
  – Semantics
• Example

• Further reading

Further reading

• Abuse cases [McDermott and Fox, 1999]
• Quality requirements
  – Safety related concerns [Sindre, 2007]
• Applications of misuse cases
  – Trade-off analysis of
    • Conflicting requirements [Alexander, 2002]
    • Secure software architectures
      [Pauli and Xu, 2005; Xu and Pauli, 2006]
  – Control scenario analysis [Hartong et al., 2006]
  – Test reusability of threat model [Jensen et al., 2010]
• Executable misuse cases [Whittle et al., 2008]
Further reading

- **Misuse cases and other techniques**
  - Combination of misuse cases and CC criteria for specification model [Choi et al., 2006]
  - Graphical vs textual misuse cases for safety hazard identification [Stålhane and Sindre, 2008]
  - Misuse cases and attack trees [Opdahl and Sindre, 2009; Karpati et al., 2014]
  - Combination of misuse cases and system architecture diagrams [Karpati et al., 2010]

Summary

- Use and misuse cases
- Security risk management
  - Abstract and concrete syntax
  - Semantics
- Example
- Further reading