Lecture 2:
Security Modelling

Understanding security goals and secure business activities

Dr. Raimundas Matulevičius
email: rma@ut.ee

Security Risk Management Domain Model
Goals and Questions

- What is modelling?
- What is Tropos
  - Secure Tropos
  - Security Risk-aware Secure Tropos
- What is BPMN
  - Security risk-oriented BPMN

What is Modelling?
Modelling…

- Modelling can guide elicitation:
  - It can help you figure out what questions to ask
  - It can help to surface hidden requirements
    - i.e. does it help you ask the right questions?

- Modelling can provide a measure of progress:
  - Completeness of the models -> completeness of the elicitation (?)
    - i.e. if we’ve filled in all the pieces of the models, are we done?

- Modelling can help to uncover problems
  - Inconsistency in the models can reveal interesting things…
    - e.g. conflicting or infeasible requirements
    - e.g. confusion over terminology, scope, etc
    - e.g. disagreements between stakeholders

- Modelling can help us check our understanding
  - Reason over the model to understand its consequences
    - Does it have the properties we expect?
  - Animate the model to help us visualise/validate the requirements

Systems involves a lot of modelling

- A model is more than just a description
  - it has its own phenomena, and its own relationships among those phenomena.

  - The model is only useful if the model's phenomena correspond in a systematic way to the phenomena of the domain being modelled

Source: Adapted from Jackson, 1995, p120-122

For every B, at least one P exists such that R(P, B)
“It’s only a model”

- There will always be:
  - phenomena in the model that are not present in the application domain
  - phenomena in the application domain that are not in the model

- A model is never perfect
  - “If the map and the terrain disagree, believe the terrain”
  - Perfecting the model is not always a good use of your time...

Source: Adapted from Jackson, 1995, p124-5

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>BPMN</td>
<td>i* (actor and goal modelling)</td>
<td>KAOS (goals for software spec.)</td>
<td>Use cases</td>
<td>Activity diagrams</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Class diagrams</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Component diagrams</td>
</tr>
</tbody>
</table>
### Security Modelling Languages

<table>
<thead>
<tr>
<th>Security Risk-oriented BPMN</th>
<th>Secure TROPOS</th>
<th>KAOS extension to security</th>
<th>Mal-activity diagrams</th>
<th>UMLsec</th>
<th>SecureUML</th>
</tr>
</thead>
</table>

#### 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>Security Risk-oriented BPMN</td>
<td>Secure TROPOS</td>
<td>KAOS extension to security</td>
<td>Mal-activity diagrams</td>
<td>UMLsec</td>
</tr>
</tbody>
</table>
Goal modelling

- **Approach**
  - Focus on *why* a system is required
  - Use goal refinement to arrive at specific requirements
  - Goal analysis
    - document, organize and classify goals
  - Goal hierarchies show *refinements* and *alternatives*

- **Advantages**
  - Reasonably intuitive
  - Explicit declaration of goals provides sound basis for conflict resolution

- **Disadvantages**
  - Captures a static picture - what if goals change over time?
  - Can regress forever up (or down) the goal hierarchy

- **Goals:**
  - Describe functions that must be carried out

- **Actors:**
  - Owners of goals

- **Tips:**
  - Multiple sources - better goals
  - Associate stakeholders with each goal
  - Use scenarios to explore how goals can be met

---

Tropos Constructs

[Diagram showing Tropos constructs with various nodes and arrows indicating relationship and flow.]
Tropos Constructs

Actor

Contribution
Means-Ends
Decomposition

satisfies
restricts
attacks
Satisfies relationship
Restricts relationship
Attacks relationship

(S) Secure (hard)goal
(S) Secure plan

Security constraint
Threat

Hardgoal
Softgoal
Plan
Resource
Secure Tropos

- **Security constraint**
  - Restriction related to the security of the system
  - Influence the analysis and design of a system
  - Restricts alternative design solutions

- **Secure dependency**
  - Introduces security constraint(s) that must be fulfilled for the dependency to be satisfied

Security risk management process
Context and Assets Identification

- Description of organisation and its environment
  - sensitive activities related to information security

Security Objectives Determination

- Determine the security objectives to be reached
  - Confidentiality, Integrity, Availability
Risk Analysis and Assessment

- Identify risks and estimate them qualitatively or quantitatively
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>

Security Requirements Definition

- **Security requirements** - security solutions to mitigate the risks

- If security requirements are unsatisfactory
  - Revise the risk treatment step
  - Revise all of the preceding steps
Control Selection and Implementations

- Implement system countermeasures within organisation

Business Process Modelling

- **Approach**
  - What organisation needs to do to achieve their business objectives?

- **Advantages**
  - Reasonably intuitive
  - Explicit declaration of business activities, processes and sub-processes

- **Disadvantages**
  - Captures only a dynamic picture
  - Not focussed on the business support by technology
Business Process Model and Notation
version 2.0

- Descriptive Modelling
- Analytical Modelling
- Executable Modelling

Business Process Model and Notation
Simple example
Asset identification //
Security objectives determination
Risk Analysis

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>
Security Requirements Definition

- Security requirements - security solutions to mitigate the risks

  - If security requirements are unsatisfactory
    - Revise the risk treatment step
    - Revise all of the preceding steps

Control Selection and Implementation
Message to take home

• Security Modelling
• Security Modelling Languages
  – Security risk-aware Secure Tropos
  – Security risk-oriented BPMN
  – Misuse cases
  – Mal-activity diagrams