Chapter 6: Security Risk-Aware Secure Tropos

Raimundas Matulevičius

University of Tartu, Estonia, rma@ut.ee
Goal

• Explain how security risks can be captured through organisation’s goals
• Understand how security risk management could be performed using Secure Tropos
Outline

• Tropos and Secure Tropos
• Security risk management
  – Abstract and concrete syntax
  – Semantics
• Example
• Further reading
Outline

• Tropos and Secure Tropos
  • Security risk management
    – Abstract and concrete syntax
    – Semantics
  • Example
  • Further reading
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 hierarchy
    - Refinements and alternatives
- **Advantages**
  - Reasonably intuitive
  - Explicit declaration of goals provides sound basis for conflict resolution
- **Disadvantages**
  - Captures a static picture
  - Can regress forever up (or down) the goal hierarchy
Goal modelling
Goal modelling

- Early requirements
- Late requirements
- Architecture design
- Detailed design
Tropos Constructs

- Actor
- Contribution
- Means-Ends
- Decomposition

Dependency relationships:
- Hardgoal
- Softgoal
- Plan
- Resource
Secure Tropos Constructs

- Actor
- Contribution
- Means-Ends
- Decomposition
- Satisfies relationship
- Restricts relationship
- Attacks relationship
- (S) Secure (hard)goal
- (S) Secure plan
- Security constraint
- Threat
- Hardgoal
- Softgoal
- Plan
- Resource
Secure Tropos
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
Outline

• Tropos and Secure Tropos
• Security risk management
  – Abstract and concrete syntax
    – Semantics
• Example
• Further reading
Abstract and Concrete syntax

Actor model
Abstract and Concrete syntax

Actor model

[Diagram of the actor model with classes and relationships including Dependum, Dependency, Secure_Dependency, Goal, Plan, Resource, Actor, Depender_SC, and Dependee_SC. Relationships are indicated with arrows, and constraints are shown in the Security_Constraint class.]
Abstract and Concrete syntax

Actor model

- Dependum
  - {complete, disjoint}

- Goal
- Plan
- Resource
  - {incomplete, disjoint}

- Softgoal
- Hardgoal

- Dependence
  - dependee
  - depender
  - restricts

- Security_Constraint
  - Depender : String [0..1]
  - Dependee : String [0..1]

- Depender_SC
- Dependee_SC

- Secure_Dependence
  - belongsTo

© Springer International Publishing AG 2017
Abstract and Concrete syntax

Actor model

[Diagram of actor model with classes and relationships]
Abstract and Concrete syntax

Actor model
Abstract and Concrete syntax

Goal model
Abstract and Concrete syntax

Goal model
Abstract and Concrete syntax

Goal model
Abstract and Concrete syntax

Relationships to Security Constraints
Abstract and Concrete syntax

Relationships to Security Constraints

© Springer International Publishing AG 2017
Abstract and Concrete syntax

Relationships to Security Constraints
Abstract and Concrete syntax

Relationships to Security Constraints
Abstract and Concrete syntax

Relationships to Security Constraints

© Springer International Publishing AG 2017
Abstract and Concrete syntax

Relationships in Attack Scenario
Abstract and Concrete syntax

Relationships in Attack Scenario

© Springer International Publishing AG 2017
Abstract and Concrete syntax

Relationships in Attack Scenario
Abstract and Concrete syntax

Relationships in Attack Scenario

- Target
  - vulnerabilityPoint : Boolean [0..1]

- Exploits

- Attacks

- Plan

- Hardgoal

- Actor
  - attacker : Boolean [0..1]

- Resource

- Goal

- explicts

- attacks

© Springer International Publishing AG 2017
Abstract and Concrete syntax

Relationships in Attack Scenario
Outline

• Tropos and Secure Tropos
• Security risk management
  – Abstract and concrete syntax
  – Semantics
• Example
• Further reading
<table>
<thead>
<tr>
<th>ISSRM concept</th>
<th>Constructs or their composition</th>
<th>Concrete syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assets</td>
<td>1) Actor, Hardgoal, Plan, Resource, Secure Goal</td>
<td>![Diagram 1]</td>
</tr>
<tr>
<td>IS assets</td>
<td>2) Composition of the construct (1) using Dependency, Means-ends, Contribution and Decomposition relationships</td>
<td>![Diagram 2]</td>
</tr>
<tr>
<td>Business assets supports</td>
<td>Relationships: Dependency, Means-ends, Contribution and Decomposition</td>
<td>![Diagram 3]</td>
</tr>
<tr>
<td>constraint of</td>
<td>Implicitly: In the Secure Dependency link Security constraint restricts (is a constraint on) a dependendum</td>
<td>![Diagram 5]</td>
</tr>
<tr>
<td></td>
<td>Explicitly: Restricts link between Security constraint and Plan, Resource, and Goal</td>
<td>![Diagram 6]</td>
</tr>
</tbody>
</table>
### Risk-related concepts

<table>
<thead>
<tr>
<th>ISSRM concepts</th>
<th>Secure Tropos</th>
<th>Constructs or their composition</th>
<th>Concrete syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat agent</td>
<td>Agent</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attack method</td>
<td>Plan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>uses</td>
<td>Agent executes Plan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat</td>
<td>Goal, Plan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerability</td>
<td>Vulnerability is not modelled, but vulnerability points can be identified by the attributes of the assets</td>
<td></td>
<td></td>
</tr>
<tr>
<td>exploits</td>
<td>Exploits</td>
<td></td>
<td></td>
</tr>
<tr>
<td>characteristic of</td>
<td>An attribute of the vulnerable asset (presented as Hardgoal, Plan, Resource)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>targets</td>
<td>Attacks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk-related concepts</td>
<td>ISSRM concepts</td>
<td>Constructs or their composition</td>
<td>Concrete syntax</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------</td>
<td>---------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Event</td>
<td>1) Composition of an Actor, Goal, Plan, Targets, Exploits, and Vulnerability point</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2) Threat</td>
<td>1)</td>
<td></td>
</tr>
<tr>
<td>Impact leads to harms</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>negates</td>
<td>1) Goals</td>
<td>2) Threats imparts</td>
<td></td>
</tr>
<tr>
<td>provocates</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk</td>
<td>Composition of a Threat and Impacts relationship</td>
<td></td>
<td></td>
</tr>
<tr>
<td>significance assessed by</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Risk treatment-related concepts

<table>
<thead>
<tr>
<th>ISSRM concepts</th>
<th>Secure Tropos</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Constructs or their composition</td>
</tr>
<tr>
<td>Risk treatment</td>
<td>—</td>
</tr>
<tr>
<td>intention to treat</td>
<td>—</td>
</tr>
<tr>
<td>Security requirement</td>
<td>1) Actor, goal, plan, resource, softgoal, security constraint</td>
</tr>
<tr>
<td></td>
<td>2) Components constructed when combining constructs (1) using dependency, means-ends, contribution and decomposition relationships</td>
</tr>
<tr>
<td>Controls</td>
<td>refines —</td>
</tr>
<tr>
<td></td>
<td>mitigates <em>Mitigates</em></td>
</tr>
<tr>
<td></td>
<td>implements Implicitly in the process of modelling</td>
</tr>
</tbody>
</table>
Outline

• Tropos and Secure Tropos
• Security risk management
  – Abstract and concrete syntax
  – Semantics

• Example

• Further reading
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 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
Outline

• Tropos and Secure Tropos
• Security risk management
  – Abstract and concrete syntax
  – Semantics
• Example

• Further reading
Further reading

• Trust, delegation, provisioning, and ownership [Giorgini et al., 2005]

• Goal risk-driven assessment [Asnar et al., 2011]

• Three-layer security analysis framework [Li and Horkoff, 2014]

• Socio-technical system development [Dalpiaz et al., 2016]

Swedbank employees' technical thesis award

Summary

• Tropos and Secure Tropos
• Security risk management
  – Abstract and concrete syntax
  – Semantics
• Example
• Further reading