TR.BPMN-1: BPMN pool is translated to the Secure Tropos actor.
TR.BPMN-2: In Secure Tropos dependencies between actors are defined following the BPMN messages flows.
TR.BPMN-3: BPMN task is defined as plan in Secure Tropos model.
TR.BPMN-4: BPMN event is defined as hardgoal in Secure Tropos model.
TR.BPMN-5: BPMN data object and data store are translated to resource in Secure Tropos model.
TR.BPMN-6: BPMN lock construct and its associated comment are translated to the Secure Tropos security constraint. The restrict relationship is defined from the security constraint to the appropriate construct.
TR.BPMN-7: BPMN pool that presents the threat agent is translated to the Secure Tropos (malicious) actor.
TR.BPMN-8: BPMN plans and message flows, used to describe the attack method are transformed to plans and situated within the malicious actor boundary in Secure Tropos model.
TR.BPMN-9: BPMN vulnerability construct is translated to the vulnerability point and placed to the exploited constructs in Secure Tropos model.
TR.BPMN-10: BPMN task that present the security requirement is transformed to the Secure Tropos secure plan.
**TR.BPMN-1:** BPMN pool is translated to the Secure Tropos role.

**TR.BPMN-2:** In Secure Tropos dependencies between actors are defined following the BPMN messages flows.

**TR.BPMN-3:** BPMN task is defined as plan in Secure Tropos model.

**TR.BPMN-4:** BPMN event is defined as hardgoal in Secure Tropos model.

**TR.BPMN-5:** BPMN data object and data store are translated to resource in Secure Tropos model.

**TR.BPMN-6:** BPMN lock construct and its associated comment are translated to the Secure Tropos security constraint. The restrict relationship is defined from the security constraint to the appropriate construct.

**TR.BPMN-7:** BPMN pool that presents the threat agent is translated to the Secure Tropos (malicious) actor.

**TR.BPMN-8:** BPMN plans and message flows, used to describe the attack method are transformed to plans and situated within the malicious actor boundary in Secure Tropos model.

**TR.BPMN-9:** BPMN vulnerability construct is translated to the vulnerability point and placed to the exploited constructs in Secure Tropos model.

**TR.BPMN-10:** BPMN task that present the security requirement is transformed to the Secure Tropos secure plan.
Goals

• Capture the security concerns using different modelling languages
  – Representations familiar to the various stakeholders
  – No need to learn new notation

• Ensure systematic and consistent security engineering process through different development stages
  – Maintain traceability

• Enhance the security model of the considered system
Outline

• Transformation Basis
  • Transformation Method
  • Comparison of Modelling Languages

• Transforming *from*
  • Security Risk-Oriented BPMN to Security Risk-Aware Secure Tropos
  • Security Risk-Aware Secure Tropos to Security Risk-Oriented Misuse Cases

• Security Risk-Oriented Misuse Cases *to*
  Mal-activities for Security Risk Management

• *What’s next?*

• Further Reading

© Springer International Publishing AG 2017
Outline

• Transformation Basis
  • Transformation Method
  • Comparison of Modelling Languages
• Transforming
  • Security Risk - Oriented BPMN to Security Risk - Aware Secure Tropos
  • Security Risk - Aware Secure Tropos to Security Risk - Oriented Misuse Cases
• Transforming
  • Security Risk - Oriented Misuse Cases to Mal-activities for Security Risk Management

• What’s next?
• Further Reading

© Springer International Publishing AG 2017
TR.MUC-MAL.1: A system boundary that presents software system in the misuse case diagram is translated to the swimlane in Mal-activities.

TR.MUC-MAL.2: A (mis)use actor is translated to the swimlane in Mal-activities.
TR.MUC-MAL.3: A **use case** construct is translated to the **activity** construct.
TR.MUC-MAL.4: The (mis)use case *security constraint* is translated to the (mal)activity *security constraint*.
TR.MUC-MAL.5: The *misuser* is translated to the *mal-swimlane*.
TR.MUC-MAL.6: The *misuse case* construct is translated to the *mal-activity*.
TR.MUC-MAL.7: The misuse case vulnerability is translated to the mal-activity vulnerability.
TR.MUC-MAL.8: A **security use case** is translated to **mitigation activity** in mal-activities.
Transformation Rules

TR.MUC-MAL.1: A system boundary that presents software system in the misuse case diagram is translated to the swimlane in Mal-activities.

TR.MUC-MAL.2: A (mis)use actor is translated to the swimlane in Mal-activities.

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

TR.MUC-MAL.4: The (mis)use case security constraint is translated to the (mal)activity security constraint.

TR.MUC-MAL.5: The misuser is translated to the mal-swimlane.

TR.MUC-MAL.6: The misuse case construct is translated to the mal-activity.

TR.MUC-MAL.7: The misuse case vulnerability is translated to the mal-activity vulnerability.

TR.MUC-MAL.8: A security use case is translated to mitigation activity in mal-activities.
Needs to be defined

- **swimlanes** to present *attack method* and *control*;
- under which **swimlanes** transformed *activities* and *mal-activities* need to be situated;
- relationships (i.e., *flows*) to define the sequences among *activities, mal-activities*, and *security activities*;
- **security constraint** and **vulnerability** places in the model.
Summary

• Transformation Basis
  • Transformation Method
  • Comparison of Modelling Languages

• Transforming from
  • Security Risk-Oriented BPMN to Security Risk-Aware Secure Tropos
  • Security Risk-Aware Secure Tropos to Security Risk-Oriented Misuse Cases
  • Security Risk-Oriented Misuse Cases to Mal-activities for Security Risk Management

• What’s next?

• Further Reading

© Springer International Publishing AG 2017