Exercises-4

Submission requirements

- Solutions should be submitted using course Website, please use - **Upload function**
- Solution file should be in **PDF** format.
- There should be authors **name** and **surname** indicated in the submission file (written on the solution sheet).
- For the valid submission at least **50%** of solutions for each exercise set should be submitted. **Grade '0' will be given if any of these requirements is not fulfilled.**
- Exercise deadline - **23:59, Tuesday** (of next week after lecture/practicals), i.e., **15th of March.**
  **In case of the late submission - a penalty of half evaluation points will be applied.**

Exercise Introduction

During lecture 2 and 3 (Security Modelling) we have studied how different modelling languages could support security risk management. We have analysed four modelling languages – Security Risk-oriented BPMN, Security Risk-aware Secure Tropos, Security Risk-oriented Misuse Cases and Mal-Activities for Security Risk Management. All these languages are aligned to the domain model of the security risk management. This also means that all these languages share the common semantics to express various concepts of the security risk management. But at the same time language limitations does not allow covering the whole concerns of the considered domain.

In these exercises you need to perform two model transformations:

- From Security Risk-aware Secure Tropos to Security Risk-oriented Misuse cases, and

Some initial literature and starting guidelines are defined in [1] and [2] (see the course Readings). Once the transformation is done you need to indicate (i) what was not captured from the input model in the new model, and (ii) what needs to be done to complete the newly received model.

Reference


Exercise 1 (40%): Transform the given Secure Tropos model to Misuse case diagram.

The following transformation rules could help to initiate the transformation:

**TR1:** An actor that presents the (software) system in Secure Tropos is translated to a misuse case software system boundary;

**TR2:** A Secure Tropos actor that presents the organisational actor (or the actor from the system environment) is translated to a misuse case actor;

**TR3:** Secure Tropos goals and plans are translated to use cases in the misuse case diagram;

**TR4:** Secure dependency links from Secure Tropos are translated to communication association in the misuse case diagram;

**TR5:** Secure Tropos means-ends and decomposition links are translated to misuse case includes relationship;

**TR6:** A Secure Tropos actor who exploits and/or targets elements of other actors, is translated to the misuser in the misuse case diagram;

**TR7:** Secure Tropos goals and plans that belong to the actor who exploits and/or targets constructs of other actors, are translated to the misuse cases in the misuse case diagram;

**TR8:** A Secure Tropos exploits relationship is translated to a threatens relationship in the misuse cases diagram;

**TR9:** A Secure Tropos mitigates link is translated to a mitigates relationship in the misuse cases diagrams.

![Diagram](image)

**Fig. 1.1.** Asset Modelling (an extract from of the Football Federation case)
Fig. 1.2. Risk Modelling (an extract from of the Football Federation case)

Exercise 2 (5%): Which concepts (complete or incomplete) of security risk management were not captured from the Secure Tropos model?

Exercise 3 (5%): Which concepts of security risk management need to be defined to complete the newly developed security risk-oriented misuse case model?
Exercise 4 (40%): Transform the current Misuse case diagram to Secure Tropos model.

The following transformation rules could help to initiate the transformation:

**TMS1.** A system boundary that presents software system in the misuse case diagram is translated to the Secure Tropos actor.

**TMS2.** A use case is translated either to Secure Tropos goal or plan belonging to the boundary of the system actor. Correspondingly, an includes link is translated either to means-ends relationship (where ends is the goal and means is the plan) or to decomposition relationship (where some plan is decomposed).

**TMS3.** An actor from the misuse case is translated to a Secure Tropos actor.

**TMS4.** (i) If the system is dependee, then the communication link is translated as dependee and the use case to which the misuse case actor communicates is defined as dependum (according to TMS3) in the Secure Tropos dependency;  
(ii) If the system is depender, then the communication link is translated as dependee and the developer specify the dependum manually, since it is not possible to capture it from the misuse case diagram;  
(iii) A security constraint could be defined to restrict the goal/plan (as well as the dependum). The restricted goal/plan is translated from the use case, to which the actor communicates in the misuse case diagram.

**TMS5.** A misuser is translated to Secure Tropos actor. In the discussion below we recall this actor as a threat agent.

**TMS6.** A misuse case is translated to the plan of threat agent. Using TMS2, an includes link is translated to the Secure Tropos decomposition relationship.

**TMS7.** A threatens relationship is translated to the Secure Tropos exploits link. The exploits link is pointed to the vulnerability point, which needs to be added to the appropriate Secure Tropos construct.

**TMS8.** A mitigates relationship from the misuse case diagram is translated to the mitigates link in Secure Tropos.

---

Fig. 2.1: Asset Modelling (an extract from the Football Federation case)
Exercise 5 (5%): Which concepts (complete or incomplete) of security risk management were not captured from the Misuse Case model?

Exercise 6 (5%): Which concepts of security risk management need to be defined to complete the newly developed security risk-aware Secure Tropos model?