**Oblig II - Security Analysis of the TaskSolver**

Conduct a security risk analysis in CORAS on behalf of a task initiator. I.e., the task initiator is the stakeholder on whose behalf the analysis is conducted. The task initiator is worried about how well his privacy is protected in the TaskSolver.

**Areas of concern**

Below is a list of topics that you can use as a starting point when identifying risks. You may also consider other topics.

1. Information flow
    a. Is it possible for an adversary to use system output (i.e., error messages, request replies etc.) plus his knowledge of the system to deduce:
        i. when another person is in a meeting?
        ii. with whom another person is meeting?
        iii. what a meeting of others is about?
2. Crafted messages
    a. Can an adversary for example obtain information about all meetings in the system by sending a crafted message?
    b. What happens if an invalid request is made?
3. Transparency
    a. Can and adversary find out about other peoples meetings just by knowing their names?
    b. Can he find out where they are going to meet?
    c. Are meeting titles visible to non-participators?
4. Backdoors
    a. What type of information is available to IT-personnel (system operators)
5. Error handling
    a. What happens if the system crashes before an agreement to meet is completed? (how is the temporary information stored?)

You should use the seven steps of the BT Technology Journal article as a basis for the risk analysis. These steps describe the procedure for a full security analysis using the CORAS method. For this exercise you only need to use a subset of the full method. The diagrams should be prepared in the CORAS editor. Your answer should include the following:

**Steps 1 to 3 – identify target of analysis etc.**

- Define the target of analysis. By target of analysis we mean the parts of the system that are included in the analysis.
  Motivate the definition. Note that it may be necessary to include system aspects that are not covered by the system diagrams from part 1 of Oblig II.
- Describe the focus of the analysis. By focus we mean the main concerns of the client, what does he want to protect and what is he worried about?
- Answer the following:
  Which of the following assets are of relevance for the analysis?
    a) The task initiators privacy

b) Confidentiality of personal data
c) The task initiators reputation
d) The task initiators safety
e) The reputation of the TaskSolver provider
f) The clientele of the TaskSolver provider

- Which of the relevant assets can be considered direct assets and which can be considered indirect assets?

  Explain your answer.
- Pick at least two relevant assets and document these in an asset diagram. You are free to identify additional assets that you think are relevant for the analysis.
- Define a consequence scale for the identified assets
- Define a likelihood scale
- Define risk evaluation criteria for each asset by means of risk evaluation matrixes. The matrixes should have two criteria:
  a) Acceptable
  b) Unacceptable

**Step 4 – risk identification**

- Select at least two of the topics under areas of concern, as a basis for identifying risks with regard to the identified assets. You may also consider other topics.
- Identify unwanted incident towards the identified assets that are relevant for the selected topics.
- What or who are the threats with regard to the selected topics?
- Consider how these threats can initiate threat scenarios leading to the unwanted incidents. Document your findings in a CORAS threat diagram. You may use more than one diagram if you want.

**Step 5 – risk estimation**

- Do the following for at least one path in a threat diagram:
  - Assign a frequency value to the initiate relation and probability values to the leads-to relations. Use these to compute the likelihood of the unwanted incident and document it in the threat diagram.
- Assign likelihood values to the remaining unwanted incidents and document them in the threat diagram(s).
- Assign consequence values to the unwanted incidents with regard to the affected assets and document them in the threat diagram(s).
- Answer the following:
  How many risks do the unwanted incidents in your diagrams give rise to?

**Step 6 – risk evaluation**

- Place the risks obtained from step 5 in the risk evaluation matrix.

**Step 7 – risk treatment**

- Identify treatments for the unacceptable risks (if any) and document these in a treatment diagram. You may use more than one treatment diagram.