SA - Phase III – Privacy analysis

This document describes phase III of the assignment. In this phase, you will analyze the privacy of the ReMeS architecture, which was created during phase II.

The privacy analysis methodology to be applied is LINDDUN, which is a privacy threat analysis framework. The LINDDUN methodology is explained in the tutorial paper, which is, together with the overview of the different privacy threat trees, available on the privacy threat tree catalog website [1]. On Toledo you will find a set of slides explaining the LINDDUN methodology and a thorough example (patient monitoring system). You are strongly advised to refer to and use this material. Also make sure you time all steps thoroughly using the Kimai time tracking tool[2].
Starting point: The architectural documentation you can start from is available on Toledo.

The deadline to turn in your report is May 14 at noon. Upload a self-contained PDF document including readable pictures and page numbers. Also, provide a printed copy.

1 Time tracking

Whenever you are working on this project, you should track the time you spend. To this aim, use the time tracking tool [2]
Four tasks will be available:

1. DFD creation
2. Mapping
3. Eliciting threats
4. Prioritization

These tasks will map to the different steps of the methodology you have to follow. A distinction has been made between *individual* work (e.g. when you are working on the assignment on your own) and *team* work, when you are collaborating with your project partner (e.g. in the lab). In the second case, only one member should log the joined time you spend on the project. **Note that it is important that you precisely track the time you spend on a specific task. Even if you take a short break, you should pause the time tracking.**

When starting with another task, first make sure you stopped/paused the current task (step 3 in Figure 1), before switching to a new one.

2 The assignment

The assignment is structured in four parts: questionnaire I, understanding the architecture, analyzing the privacy, and questionnaire II.

2.1 Questionnaire I

Before working on the actually assignment, you must fill in the questionnaire that is available at: `https://docs.google.com/spreadsheet/viewform?formkey=dEhiWU9fTEpMXzdUUVhobEJWZm5aLXc6MA#gid=0`

[1] See `https://people.cs.kuleuven.be/~kim.wuyts/private/SA2012/`, login using your student number and corresponding password

[2] See `http://people.cs.kuleuven.be/~kim.wuyts/SA2012/kimai`. Your username is your KULeuven student number (e.g. s0000001) and the corresponding password will be mailed to you.

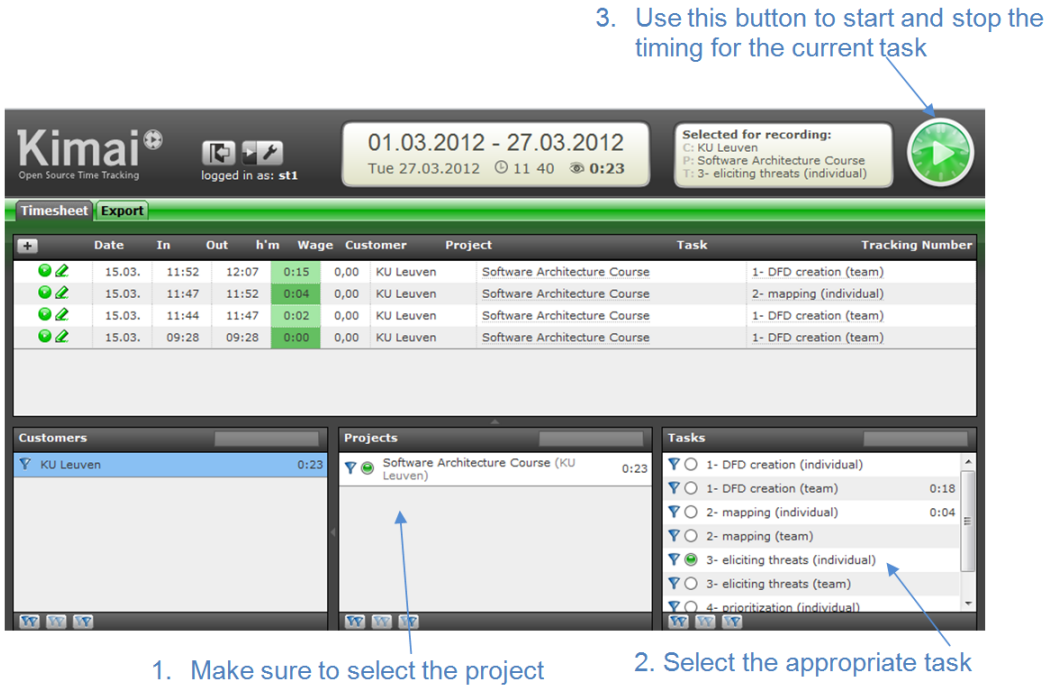

Figure 1: The Kimai time tracking tool

2.2 Understanding the architecture

The first part of the assignment focuses on understanding the architecture to be analyzed. To get familiar with the architecture, careful read the provided architectural documentation. When you believe you fully understand the documentation, test your knowledge by answering the following question:

Briefly describe (max 2-3 paragraphs) the scenario where an alarm arrives at the ReMeS back-end and the actuator is activated

Your answer should be included in the report (see below). This exercise should not be timed.

2.3 Privacy analysis

Analyze the privacy of the ReMeS system using the LINDDUN methodology.

As a reminder, the following steps need to be followed:

1. Create a DFD that represents the ReMeS architecture. The DFD's level of detail should be similar to the provided example (in the slides).
2. Map the DFD elements to the LINDDUN privacy threats according to the provided mapping table.
3. Threat elicitation
   (a) Using the provided privacy threat trees and based on the mapping created in the previous step, elicit those privacy threats that are relevant to the system
   (b) Document the privacy threats using the provided threat description template

(c) Assumptions about the systems (e.g. a certain communication link is considered encrypted) and decisions in general (e.g. non-repudiation of data flows is not considered a threat for this system, or we have combined several threats into one misuse case scenario) which influence your threat elicitation should be made explicit, as well the reasoning behind it. These assumptions will be critical for grading the elicited threat, as they will explain why a certain threat was (or was not) included.

4. Prioritize the threats you elicited and documented according to their risk (likelihood * impact). At least, you must divide them in 3 categories: high, medium, and low. If possible, you should also try within each category to order the threats according to their level of risk.

2.4 Questionnaire II

After you finished the privacy analysis, you must fill in the questionnaire that is available at: `https://docs.google.com/spreadsheet/viewform?formkey=dGhVeTVCeVFOdU5pOFBpWkR3YktBNHc6MQ#gid=0`

3 The report

The report must be structured in two sections (the exercise to get familiar with the architecture, and the actual analysis).

Your report should consist of the following sections (also see the example report and the latex templates).

3.1 Understanding the architecture

A brief description of –3 paragraphs that elaborate on the scenario.

3.2 Privacy analysis

This section should consist of 4 main parts, which correspond to the 4 steps of the LINDDUN methodology.

1. *DFD:* This section should 1) contain the DFD diagram and 2) briefly explain the choices that were made (e.g. why did you not represent a certain component, why did you represent a certain component in more detail than in the architecture, ...)

2. *DFD - threat mapping:* The mapping is represented by a table that shows the mapping of each DFD element to the LINDDUN threats

3. *Eliciting threats:* This section consists of 2 main parts:

   (a) *Assumptions:* This section lists (using a numbered list) general assumptions that are applicable to the entire system and decisions that were made which influence the elicitation process (e.g. why a certain threat is no longer considered, why several threats are combined in 1 misuse case, etc.). When a threat is based on one or more of these assumptions, you should refer to them (using the "notes" part of the threat description template).

   (b) *Threats:* This section describes the identified threats using the template which is further explained in the following section. **Make sure you list the threats in order of discovery.**

4. *Prioritization of threats:* Once all threats are described, 1) give an overview of the different threat titles and order them according to their risk. The threats must be divided in 3 categories: high, medium, and low risk. If possible, also order them according to their risk within each category. 2) Also briefly justify your order

3.2.1 Threat description template

Each threat should be structured according to the following template:

- ID (e.g. T01)
- Title)
- Summary
- Primary mis-actor(s): insider vs. outsider, skilled vs. unskilled
- Basic path
- Consequence
- Reference to leaf node(s): which leaf node(s) inspired you for this threat
- Reference to root node(s): as multiple trees can result in the same leaf node, you should enlist all root nodes that you examined and resulted in this specific threat (this list should be ordered according to discovery (latest examined root node at the end))
- Reference to DFD element(s): give the name of the DFD element(s) to which this threat applies
- Remarks: optional field which can be used to give more information about the threat (e.g. explain why this threat corresponds to different DFD elements). Here you can also include references to the assumptions if applicable.

4 Participation in experiment

We would like to remind you that some of the results of this assignment will also be used for a research study. For instance, we will use

- the time you spend on the assignment (which you self-report)
- the usage statistics of the threat tree catalog website
- the documented threats

Note that the participation to this study will have no impact on your grade. Also, your participation in the study will not create any overhead concerning the assignment.

If you have any objections against us using your data, you can opt-out by sending us (swarch-course@cs.kuleuven.be) an email by May 14.

Good luck!

The Software Architecture team.