Principles of Secure Software Design
Examination II
04.06.2020

Correctness (of used methods) and completeness (within the selected scope) will be the two major criteria to assess your solutions.

Online Room Reservation System
Based on the previous RE workshop solution

The scope of the Online Room Reservation System (ORRS) is an online web-interface for the users to check the availability and book the room from any part of the world. This system will be an alternative to the traditional offline way of checking available rooms and book them. The system will have two major types of users: customers and hotel manager. The system is used by different stakeholders for entering different details to select and reserve rooms at a hotel. For instance, customers can sort, select, and reserve a room; hotel managers can update room information and viewing reports, staff personnel can use the while preparing the rooms for the new customers; etc.

The mockup prototype of the ORRS system is available here:
<https://app.moqups.com/VxOuSI2HQ2/view/page/ad64222d5>

Tasks

Before starting with your solutions, read all the tasks. All tasks are interconnected and basically you need to define one solution by preparing answers to different tasks.

Task 1: In the given scenario define the Scope! How large is your problem? You do not need to analyze all the ORRS system (if you do so, you will not have time to complete all the tasks). Answer to this task is a written paragraph, where you explicitly state what you analyze in other tasks.

(10 points)

Task 2: Create a business process diagram using the BPMN modelling language. In other words – design your base scenario (according to the defined scope), where, for example, interactions between three or four pools (e.g., Customer, Manager, Staff personnel, and ORRS) and their activities are defined.

(20 points)

Task 3: What are the protected objects and their properties: (i) identify and write protected object(s) (and their (its) attributes); and (ii) determine and write down the security objectives.

(10 points)

In task 4 and 5 you need to define role-based access control policy using two different modelling languages.
Task 4: Define SecureUML model representing role-based access control policy regarding the scenario defined in Task 2 (and protected object in Task 3). Do not forget to show explicitly the security action model. Write at least three authorisation requirements (do not mix these with authorisation constraints, which should be a part of the SecureUML model).

(25 points)

Task 5: Define the UMLsec model representing role-based access control policy regarding the scenario defined in Task 2 (and protected object in Task 3). Write at least two authorisation requirements, different than in Task 4 (do not mix these with association tags, which should be a part of the UMLsec model).

(25 points)

Task 6: From your analysis (see tasks 1 to 5) identify one security risk and fill in Table 1.

(10 points)

Table 1: Security Risk Management template

|----------------|--------------|--------------------|------|-------|--------|--------|---------------|--------------|---------------|----------------------------------|---------------------|------------------|

In summary, the solution should include:
- For task 1: a paragraph describing problem scope;
- For task 2: business process diagram in BPMN capturing the ORRS scenario (within the scope defined in Task 1);
- For task 3: description of the protected object and security objectives;
- For task 4: SecureUML model defining RBAC policy (static perspective) and three authorisation requirements;
- For task 5: UMLsec model defining RBAC policy (dynamic perspective) and two authorisation requirements;
- For task 6: filled in security risk management template (Table 1) for one security risk.

Submission: your solution should be submitted using the course Website, Upload function. The submission will be opened until 14:20; but it is highly recommended to do submission at 14:00. Alternatively, you could email your solution to <rma@ut.ee> but your email should come no later than 14:05 (please use Subject [SSD examination]). Solution submitted / emailed after the identified deadline will not be accepted.

It is appreciated if PDF file is submitted; but other format files will also be accepted. In case of several files, please archive (e.g., zip) all files.

You can use all material (e.g., course Website, course book), but the solutions must be prepared individually.