Creativity – your key to secure software!!!

Student name and surname: ____________________________

Student ID: __________________________________________

EXAMINATION

The exam is open-book, open-laptop, and open-Internet. You are not allowed to share information or discuss with anyone during the exam other than the lecturer. You can provide your solutions either on paper or electronically. In case of the electronic solutions, please email the file to < rma@ut.ee > with subject “[SSD2018] exam solutions”. Your email should reach me by 16:05 the latest.

Scenario

During the course one of the illustrative examples was the xRoad system used in Estonia. As it was discussed, it contains a lot of concerns related to the software system security. Following this example prepare solutions to the given tasks.

General:

• All security risks (presented textually or graphically) should be grounded using the taxonomies (for threat agent, attack method, threat, vulnerabilities, and impacts, see lecture 2 for more detailed reference).
• Security requirements (presented textually or graphically) should correspond to the “criteria of good requirements” (see lecture 2 for more detailed reference).
• Major evaluation criteria are completeness, correctness and consistency of the solution within the defined scope of the xRoad system.

TASKS

Task 1. What is an xRoad system? What are its products/components? What are its infrastructure and applications? Who are information technology staff, internal users and managers, and customers and external users? What is its environment?

(10 points)

Task 2: What are the valuable business assets (at least 2) and security criteria of the xRoad system? What are the system assets that support each identified business asset? Explain how these system assets support the business assets.

(10 points)

Task 3: Define one security risk to the asset or asset group (see Task 2)? Consider the following questions: what is the vulnerability(-ies) of the system asset(s)? Who is a threat agent? What is the security threat that targets the system asset(s)? What is the risk impact(s)? How does the impact harm the business asset and the system asset? How does this impact negate the security criteria?

(15 points)
Task 4: In order to mitigate risk identified in Task 3, what is the security risk treatment decision? What are the security requirements and how could they be implemented? (10 points)

Task 5: Select one modelling language from security risk-oriented business process model and notation, security risk-oriented misuse cases or mal-activities for security risk management; create the visual model representing security risk defined in Task 3. (10 points)

Task 6: If you have selected security risk-oriented misuse cases or mal-activities for security risk management, define a set of transformation rules to translate the modelling language selected in Task 5 to security risk-aware Secure Tropos. If you have selected security risk-oriented business process model and notation, define a set of transformation rules to translate its models to security risk-oriented misuse cases. (10 points)

Task 7: Apply the defined transformation rules (task 6) to translate the security risk model (see Task 5). Discuss what was not possible to translate using your transformation rules. (15 points)

Task 8: Create a visual security risk treatment model (see task 4). Use any (one) language of the two considered in Task 6. (10 points)

Task 9: There exist different roles participating in the xRoad processes. Define a role-based access control policy. To solve this task apply the SecureUML modelling language. (10 points)

Task 10: Extract authorisation requirements (at least 4) from the model defined in Task 9. (10 points)

Task 11: If you need to develop a new xRoad system, which system development lifecycle would you apply? What techniques, methods, tools, etc. for security engineering would you apply at each stage of this lifecycle? (10 points)