EXAM TASKS

[The sum of points equals to 110]

During the course of the Principles for Secure Software Design one of the illustrative industrial examples was the X-Road the backbone of the Estonian governmental Information system. It is a system for securing the inter-organisational data exchange. It is not a physical communication network, but more like VPN with digital signatures and access control for web-services. As it was discussed during the lecture, this system contains a lot of concerns related to the software system security. Following this example prepare solutions to the given tasks.

Part I. Security Risk Management

[You will be evaluated for the semantic precision of the given solutions.]

Task 1: Content and asset identification
What are the valuable business assets (at least 3) of the X-ROAD system? What are the system assets that support each identified business asset? Explain how these system assets support the business assets.

[5 points]

Task 2: Determination of security objectives
What are the security criteria (in terms of confidentiality, integrity, and availability) for each identified business asset? Please explain your answer.

[5 points]

Task 3: Risk analysis and assessment
What are security risks to the defined assets? To complete this task, it is enough to define only one security risk to the selected asset (or their group) identified in task 1. When defining the risk, consider these questions:
- What is the vulnerability(-ies) of the system asset(s)?
- What is the security threat that targets the system asset?
- 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?

[10 points]

Task 4: Security risk treatment decision
What is the security risk treatment decision to the identified risk? What is a potential alternative risk treatment decision? Please explain your answer.

[5 points]

Task 5: Security requirements definition
What are the security requirements that mitigate the identified risk? You need to define at least 4 security requirements that refine (either primary or alternative) risk treatment decision. Each security requirement should:
- specify what (not how) should be done to mitigate the risk;
- be understandable;
- be cohesive;
- be testable.

[10 points]
Creativity – your key to secure software!!!

Task 6: Control selection and implementation
Discuss briefly, how the identified security requirements could be implemented to the security controls (or what security controls implement the defined requirements).

Part II. Security Modelling
[You will be evaluated for the syntactic precision and application of the selected modelling language.]

Select one security risk-oriented modelling language; for example, you can choose among Secure Tropos, Misuse cases, Mal-activity diagrams, BPMN extended to security or similar. For your solution to Part I:

Task 7: Create a diagram that represents problem content and (both business and system) assets including their security criteria, elicited in Tasks 1 and 2.

Task 8: Create a diagram that represents the security risk elicited in Task 3.

Task 9: Create diagram that represents security requirements, elicited in Task 5 (also if, language expressiveness allows, security controls) and show these requirements mitigate the security risk.

Part III. Role-based Access Control
[You will be evaluated both for the semantic and syntactic correctness of the modelling language application.]

Task 10: As discussed during the x-road lecture, at least four major roles (i.e., service providers, service consumers, x-road citizens, and x-road central agency) participate during the election process. Define a role-based access control policy to some provided service in X-Road. To solve this task apply the SecureUML modelling language.
Creativity – your key to secure software!!!

Part IV. Bonus – Multiple Choice Questionnaire

[Each correctly answered question gives you 1 point.]

Q1. Which attack methods could be used by threat agents to break into the system?

   a) SQL injection attack;
   b) Pre-texting or phishing;
   c) Seamless installation of the key-loggers;
   d) Cross-site scripting attack;
   e) All a, b, c, and d;
   f) Neither a, b, c, nor d.

Q2. **Trust** is defined as an expectation of one actor about the behaviour of another actor by whom he might be positively or negatively affected. Which of these statements are correct?

   a) Trustworthiness is a characteristic of the trustee;
   b) Trust is a characteristic of the trustor;
   c) Trustworthiness is a characteristic of the trustor;
   d) Trust is a characteristic of the trustor;
   e) All a, b, c, and d;
   f) Neither a, b, c, nor d.

Q3. How is the potentiality of risk event estimated?

   a) Estimated as a sum of threat likelihood and vulnerability level;
   b) Estimated as maximum impact level of concerned impacts;
   c) Estimated as security needs (the same method, just reversed thinking);
   d) Estimated from the security needs;
   e) All a, b, c, and d;
   f) Neither a, b, c, nor d.

Q4. Which security problems could be caused by the API abuse?

   a) Directory restriction;
   b) Trust boundary violation;
   c) Privacy violation;
   d) Setting manipulation;
   e) All a, b, c, and d;
   f) Neither a, b, c, nor d.

Q5. What are identification requirements?

   a) When application protects itself from infection by unauthorised programs;
   b) When business keeps its sensitive data private from unauthorised use;
   c) When application ensures that its data are not intentionally corrupted;
   d) When business shall identify its externals before interacting;
   e) All a, b, c, and d;
   f) Neither a, b, c, nor d.
Creativity – your key to secure software!!!

Q6. What are misuse cases?
   a) It is a security modelling technique;
   b) They describe what the system should do to meet the objectives;
   c) They describe what the system should avoid from doing;
   d) They describe what the systems should do related to the threats;
   e) All a, b, c, and d;
   f) Neither a, b, c, nor d.

Q7. What is an RBAC user?
   a) Any person who interacts with a system;
   b) A relationship among roles;
   c) An entity that causes information to flow;
   d) A specific type of interaction between a subject and an object;
   e) All a, b, c, and d;
   f) Neither a, b, c, nor d.

Q8. Which RBAC functionality should be supported, after user assignments and permission assignments are defined?
   a) View session roles and permissions
   b) Transformation of SecureUML diagram to UMLsec;
   c) Creation of sessions and checking the access;
   d) View of assigned users, roles and their permissions;
   e) All a, b, c, and d;
   f) Neither a, b, c, nor d.

Q9. What is shoulder surfing?
   a) Pawing through a target’s garbage in search of valuable information;
   b) Stealth observation of the target to obtain or deduce confidential information;
   c) Exploiting user’s curiosity to deliver malware;
   d) Continuing to function even if a data centre is destroyed;
   e) All a, b, c, and d;
   f) Neither a, b, c, nor d.

Q10. Which of these “points” do not belong to the “Seven Security Touchpoints”?
    a) Test plans;
    b) Security requirements;
    c) Risk-based test;
    d) Penetration testing;
    e) All a, b, c, and d do not belong;
    f) All a, b, c, nor d do belong.