Principles of Secure Software Design
Examination I
30.05.2019

Correctness and completeness will be the two major criteria to assess your solutions.

<table>
<thead>
<tr>
<th>Task</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task 1</td>
<td>12</td>
</tr>
<tr>
<td>Task 2</td>
<td>16</td>
</tr>
<tr>
<td>Task 3</td>
<td>22</td>
</tr>
<tr>
<td>Task 4</td>
<td>10</td>
</tr>
<tr>
<td>Task 5</td>
<td>20</td>
</tr>
<tr>
<td>Task 6</td>
<td>15</td>
</tr>
<tr>
<td>Task 7</td>
<td>10</td>
</tr>
<tr>
<td>Test</td>
<td>30</td>
</tr>
<tr>
<td><strong>Total:</strong></td>
<td><strong>135</strong></td>
</tr>
</tbody>
</table>

Course grade 45
**Task 1:** Analyse the model given in Fig. 1. Write (potentially with some explanation) one example of each function for information processing. To support your answer, fill Table 1.

Table 1:

<table>
<thead>
<tr>
<th>Information processing function</th>
<th>Example (and explanation)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Capture information</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Transmit information</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Store information</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Retrieve information</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Manipulate information</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Display information</strong></td>
<td></td>
</tr>
</tbody>
</table>
Fig. 1: Asset modelling using Secure Tropos
Task 2: These security requirements are extracted from solutions of your colleagues. Do they correspond to the “criteria of good requirements”? If not, please refine them so that they would correspond to the “criteria of good requirements”.

SecReq.1: Automation of the receipt generation or checking fuel capacity and sold amount of fuel as often as possible.

SecReq.2: Implementing at least two workplaces for serving customers in filling station.

SecReq.3: Appropriate trainings shall be provided to all employees of PowerAB with regards to information security awareness.

SecReq.4: Database backup server accounts should be sufficiently protected against unauthorized access.

SecReq.5: After match team representatives sign the report and optionally provide comments

SecReq.6: Confirmation of game results by the team shall be allowed only for team representative which represents team under action

SecReq.7: ERIS shall allow all users to view all data in the game report.

SecReq.8: Football Federation Employee should be identified before having access to use the functions related to the creation of the game report to prevent unauthorized people to create fake game reports.
Task 3: From the security risk-oriented misuse cases model, given in Figs. 2-4 extract information and fill in Table regarding one security risk (*its related assets and security countermeasures*)

<table>
<thead>
<tr>
<th>Concepts</th>
<th>Asset, risk, and risk treatment definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business asset</td>
<td></td>
</tr>
<tr>
<td>System asset</td>
<td></td>
</tr>
<tr>
<td>Security criterion</td>
<td></td>
</tr>
<tr>
<td>Risk</td>
<td></td>
</tr>
<tr>
<td>Impact</td>
<td></td>
</tr>
<tr>
<td>Vulnerability</td>
<td></td>
</tr>
<tr>
<td>Threat agent</td>
<td></td>
</tr>
<tr>
<td>Attack method</td>
<td></td>
</tr>
<tr>
<td>Risk treatment decision</td>
<td></td>
</tr>
<tr>
<td>Security requirement</td>
<td></td>
</tr>
<tr>
<td>Control</td>
<td></td>
</tr>
</tbody>
</table>
Fig. 2. Security risk-oriented misuse cases – diagram 1

Fig. 3. Security risk-oriented misuse cases – diagram 2
Task 4: Represent security risk from Fig. 3 in one of these languages:

- Security risk-oriented BPMN;
- Security risk-aware Secure Tropos;
- Mal-activities for security risk management.

Task 5: Table 3 presents some metrics gathered regarding risks 1, 3, 6, and 7. Complete Table 3 with the missing metrics (and their calculations). Use the given graphs and fill in Table 4

Which risks are of the highest priority (highest severity)?

Write your answer to this question here:
### Table 3:

<table>
<thead>
<tr>
<th>RiskID</th>
<th>Business asset value</th>
<th>Security objective</th>
<th>Before treatment</th>
<th>After treatment</th>
<th>Risk reduction level</th>
<th>Cost of countermeasure</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Vulnerability level</td>
<td>Treat likelihood</td>
<td>Event potentiality</td>
<td>Impact level</td>
</tr>
<tr>
<td>Risk1</td>
<td>3</td>
<td>C=</td>
<td>3</td>
<td>2</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>Risk3</td>
<td>1</td>
<td>C=</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Risk6</td>
<td>3</td>
<td>C=</td>
<td>3</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Risk7</td>
<td>1</td>
<td>C=</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>1</td>
</tr>
</tbody>
</table>

### Table 4:

<table>
<thead>
<tr>
<th>Risk ID</th>
<th>Value/RRL</th>
<th>Cost/RRL</th>
<th>Value/Cost</th>
<th>Total</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Task 6: In business process diagram (see Fig. 5 a), four occurrences were identified using the SRP1 pattern (Secure data from unauthorized access).

1.1: Extract security model (for the Game business asset) using SecureUML modelling language

1.2: Derive security requirements (at least 3)

Fig. 5: (a) Business process diagram and (b) SRP1 asset model of SRP1
**Exercise 7**: How security model created in Exercise 6 should be presented using UMLsec modelling language. Correctness and completeness of the model will be assessed.
Multiple choice test

Question will be answered correctly if all correct answers are selected.

1. How are information, processes and skills inherent to the organisations business that have value to the organisation in terms of its business model and is necessary for achieving its objectives, called?
   - System asset
   - Business asset
   - Security requirement
   - Control
   - There is no correct answer

2. What is a characteristic of a system asset or a group of system assets that can constitute a weakness or a flaw in terms of system security?
   - Security criterion
   - Attack method
   - Vulnerability
   - Security requirement
   - There is no correct answer

3. What is a property or constraint on business asset?
   - Security criteria
   - Vulnerability
   - Impact
   - Security requirement
   - There is no correct answer

4. How is a decision on an action to lessen the probability, negative consequences, or both, associated with a risk, called?
   - Risk avoidance decision
   - Risk mitigation decision
   - Risk reduction decision
   - Risk treatment decision
   - There is no correct answer

5. How is an agent that can potentially cause harm to system assets called?
   - James Bond
   - Threat actor
   - Threat agent
   - Attack agent
   - There is no correct answer

6. How are attacks to communication between distributed components called?
   - Identity attacks
   - Network communication attacks
   - Passing illegal data attacks
   - Stored data attacks
   - There is no correct answer
7. How are security attacks where input data is manipulated by attacker for some malicious purpose, called?

☐ Identity attacks
☐ Passing illegal data attacks
☐ Remote information inference attacks
☐ Loss of accountability attacks
☐ There is no correct answer

8. How are threats to countermeasures which uses cryptography called?

☐ Countermeasure design threats
☐ Passing illegal data attacks
☐ Remote information inference attacks
☐ Loss of accountability attacks
☐ There is no correct answer

9. How are requirements that define the expected level of safety from the system with respect to the unintentional accidents, called?

☐ Privacy requirements
☐ Security requirements
☐ Safety requirements
☐ Survivability requirements
☐ There is no correct answer

10. How are requirements that define the extent to which a system shall be verify the identity of its externals before interacting with them, called?

☐ Immunity requirements
☐ Integrity requirements
☐ Intrusion detection requirements
☐ Survivability requirements
☐ There is no correct answer

11. How are requirements that define the extent to which a system shall be prevent authorised modifications from accidentally defeating its security mechanisms, called?

☐ Physical protection requirements
☐ survivability requirements
☐ Non-repudiation requirements
☐ Immunity requirements
☐ There is no correct answer

12. How can modelling help to check the understanding of the problem?

☐ Explain how security countermeasures can be captured through organisational goals
☐ Revise the risk treatment steps
☐ Reason over the model to understand its consequences
☐ Animate the model to help visualise/validate the requirements
☐ There is no correct answer
13. Which constructs are used to represent business assets in BPMN?

☐ Event
☐ Task
☐ Data Store
☐ Data Object
☐ There is no correct answer

14. Which construct is used to represent vulnerability in BPMN?

☐ Event
☐ Task
☐ Pool
☐ Sequence flow
☐ There is no correct answer

15. Which of the following constructs can be used to refer to vulnerability in Secure TROPOS?

☐ Hardgoal
☐ Vulnerability point
☐ Resource
☐ Vulnerability construct
☐ There is no correct answer

16. Which of the following constructs can be used to represent system assets in Secure TROPOS?

☐ Security constraint
☐ Plan
☐ Softgoal
☐ Resource
☐ There is no correct answer

17. Which of the following constructs can be used to represent system assets in Security risk-oriented misuse cases?

☐ Security Use Case
☐ Secure System Agents
☐ Misuse Case
☐ Constraint-of Relationship
☐ There is no correct answer

18. Which of the following constructs can be used to represent vulnerability in Security risk-oriented misuse cases?

☐ Vulnerability
☐ Security criterion
☐ Misuser
☐ Misuse case
☐ There is no correct answer
19. Which of the following constructs can be used to represent components of risk using Mal-activities for the risk management?

☐ Mal-swimlane
☐ Informal comment
☐ Malicious Activity
☐ Mal-decision
☐ There is no correct answer

20. Which of the following constructs can be used to represent vulnerability using Mal-activities for risk management?

☐ Decision
☐ Mitigation Activity
☐ Malicious Activity
☐ Swimlane
☐ There is no correct answer

21. What does it mean when an attacker cannot sufficiently distinguish whether two or more items of interest (from the attacker’s perspective) are related or not?

☐ Anonymity
☐ Unlinkability
☐ Undetectability
☐ Unobservability
☐ There is no correct answer

22. What does it mean when an attacker cannot sufficiently identify the subject within a set of subjects (from the attacker perspective)?

☐ Anonymity
☐ Identifiability
☐ Unobservability
☐ Pseudonymity
☐ There is no correct answer

23. How is a specific type of interaction between a subject and an object that results in the flow of information from one to another called?

☐ Access control
☐ Session
☐ Access
☐ Permission assignment
☐ There is no correct answer

24. How is an active entity that causes information to flow among objects or changes the system state called?

☐ Administrator
☐ User
☐ Subject
☐ Role
☐ There is no correct answer
25. What are patterns for enterprise security and risk management about?

☐ Threat assessment
☐ Asset valuation
☐ Role-based access control
☐ Enterprise partner communication
☐ There is no correct answer

26. What are patterns for identification and authentication about?

☐ Threat assessment
☐ PKI design alternatives
☐ Unregistered users I&A requirements
☐ Role-based access control
☐ There is no correct answer

27. Patterns for firewall architecture represent trade-offs between complexity, speed and security, which are tailored to control attacks on specific layers of the network. What are the major types of the firewall architecture patterns?

☐ Proxy-base firewalls
☐ Packet filter firewalls
☐ Address filtering lanes
☐ Stateful firewalls
☐ There is no correct answer

28. What is the input for the SREBP method?

☐ Value chain diagram
☐ Security objectives determined for business supported by the systems assets
☐ Business process diagrams
☐ Pattern occurrences identified when applying security risk-oriented patterns
☐ There is no correct answer

29. What components needs to be identified when creating role-based access control security model?

☐ Resources, roles (and users)
☐ Secured operations
☐ Permissions and security constraints
☐ Confirmations and reports
☐ There is no correct answer

30. What are the seven security touchpoints?

☐ Information systems security risk management
☐ Role-based access control
☐ Privacy-by-design
☐ Data leakage management
☐ There is no correct answer