**EXAM TASKS**

*The sum of points equals to 100*

**PART I: Security Risk Management**

**Problem description:** Telephone banking is a service provided by a financial institution, which allows its customers to perform transactions over the telephone. Most telephone banking services use an automated phone answering system with phone keypad response or voice recognition capability. The customers have to authenticate through a numeric or verbal password or through security questions asked by a live representative. With the obvious exception of cash withdrawals and deposits, telephone banking offers virtually all the features of an automated teller machine:

- account balance information;
- list of latest transactions;
- electronic bill payments;
- funds transfers between a customer's accounts.

Usually, customers can also speak to a live representative located in a call centre or a branch, although this feature is not always offered 24/7. In addition to the self-service transactions, representatives of the telephone banking are usually trained to do what is traditionally available only at the bank-branch. It includes:

- loan applications;
- investment purchases and redemptions;
- debit card replacements;
- change of address.

To secure telephone banking, some developers have applied the security patterns. One of the security risk-oriented patterns is provided in Table 1. This pattern partially describes how to secure data transmission between two system entities.

Use the security risk-oriented language (choose one among security risk-oriented BPMN, Secure Tropos, Misuse cases diagrams, or Mal-activity diagrams) and illustrate (one example is enough!) how this pattern is applied in the given context of the mobile banking.

Three diagrams needs to be created in order to show:

- **Task 1:** What are the context, assets and their security criteria; (15 points)
- **Task 2:** How does the security risk constitute itself; (20 points)
- **Task 3:** What is the countermeasure (i.e., risk treatment, security requirements, and controls), and how does it mitigate the security risk. (15 points)

**Note:** Although a picture is worth 1000 words, short textual explanations of the diagrams are welcome!
Table 1: Security risk-oriented pattern – securing data between two entities

<table>
<thead>
<tr>
<th>Assets and security objective definition</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Business assets</td>
<td>Data submitted, transmitted and employed</td>
</tr>
<tr>
<td>IS assets</td>
<td>Input interface, Transmission medium that transfers data, and Server</td>
</tr>
<tr>
<td>Security criteria</td>
<td>Integrity of data</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk definition</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk</td>
<td>An attacker intercepts the transmission medium due to its characteristics of being intercepted and misuses the data leading to loss of data integrity</td>
</tr>
</tbody>
</table>
| Impact          | - Harm data submitted and employed in server  
|                 |  - Loss of reliability of the transmission medium  
|                 |  - Negation of data integrity |
| Event           | An attacker intercepts the transmission medium due to its characteristics to be intercepted and misuses the data. |
| Threat          | An attacker intercepts the transmission medium and misuses the data. |
| Vulnerability   | - Characteristics of transmission medium to be intercepted; |
| Threat agent    | An attacker with means to intercept transmission medium. |
| Attack method   | - Intercept transmission medium by establishing a proxy between input interface and server;  
|                 |  - Misuse data by capturing, modifying and passing data to the server. |

<table>
<thead>
<tr>
<th>Risk treatment definition</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk treatment</td>
<td>Risk reduction</td>
</tr>
<tr>
<td>Security requirement</td>
<td>- Verify the received data with the original</td>
</tr>
<tr>
<td>Control</td>
<td>Checksum algorithm</td>
</tr>
</tbody>
</table>

**PART II: Model-driven Security**

**Problem description:** Alice is a security analyst at the SDO company, which is a software development organisation specialised in creating new information management solutions. In order to understand requirements for the Order Delivery System (ODS), firstly, Alice has interviewed four people: Eva, John, Jeremy, and Tom. Next, she has created a security model using UML sec modelling language (see Figure 1; Tables 2 presents the association tags; and Table 3 gives short description of few actions). However, now she needs (i) to validate the elicited security requirements with Eva, John, Jeremy, and Tom; and (ii) to prepare another model, such that SDO implementation team could generate the executable ODS.

**Task 4:** Using Figure 1 or/and model created in Task 5, help Alice to specify at least 5 ODS security requirements textually. Each requirement should say what the ODS needs to do, it should be unambiguous, cohesive and testable.

(10 points)

**Requirement ID1:** The ODS application …

**Requirement ID2:** …
Task 5: Using the SecureUML modelling language, create the class diagram, which would present the RBAC policy in correspondence to the Alice model.

The class diagram should specify:
- Protected Resource(s), its Attributes and protected Operations (10 points)
- Users, Roles, and User assignments (5 points)
- Permissions, Permissions assignment and Security actions (15 points)
- Security authorisation constraints, either in OCL or at least in plain text (10 points)
Creativity – your key to secure software!!!

Table 2: Associated tags

<table>
<thead>
<tr>
<th>{Protected = Create new order}</th>
<th>{Protected = Display order}</th>
</tr>
</thead>
<tbody>
<tr>
<td>{Role = (John, Customer)}</td>
<td>{Role = (Tom, DeliveryDepartment)}</td>
</tr>
<tr>
<td>{Right = (Customer, Create new order)}</td>
<td>{Right = (DeliveryDepartment, Display order)}</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>{Protected = Display new order}</th>
<th>{Protected = Confirm delivery}</th>
</tr>
</thead>
<tbody>
<tr>
<td>{Role = (Eva, SalesDepartment)}</td>
<td>{Role = (Tom, DeliveryDepartment)}</td>
</tr>
<tr>
<td>{Role = (Jeremy, SalesDepartment)}</td>
<td>{Role = (Jeremy, DeliveryDepartment)}</td>
</tr>
<tr>
<td>{Right = (SalesDepartment, Display new order)}</td>
<td>{Right = (DeliveryDepartment, Confirm delivery)}</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>{Protected = Mark availability status}</th>
<th>{Protected = Display customer’s order}</th>
</tr>
</thead>
<tbody>
<tr>
<td>{Role = (Eva, SalesDepartment)}</td>
<td>{Role = (John, Customer)}</td>
</tr>
<tr>
<td>{Right = (SalesDepartment, Mark availability status)}</td>
<td>{Right = (Customer, Display customer’s order)}</td>
</tr>
</tbody>
</table>

Table 3: Action description

<table>
<thead>
<tr>
<th>Action …</th>
<th>… concerns attributes…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create new order</td>
<td>(created and filled by the customer) Contact information, Delivery address, Requested item; (left with the null value, but created as part of the application) Availability status, Delivery status</td>
</tr>
<tr>
<td>Display new order</td>
<td>Delivery address, Requested item</td>
</tr>
<tr>
<td>Mark availability status</td>
<td>Availability status</td>
</tr>
<tr>
<td>Display order</td>
<td>Contact information, Delivery address, Requested item, Availability status</td>
</tr>
<tr>
<td>Confirm delivery</td>
<td>Delivery status</td>
</tr>
<tr>
<td>Display customer’s order</td>
<td>Contact information, Requested item, Availability status, Delivery status</td>
</tr>
</tbody>
</table>
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. How is the potentiality of risk event estimated?
   a) Estimated as security needs (the same method, just reversed thinking);
   b) Estimated from the security needs;
   c) Estimated as a sum of threat likelihood and vulnerability level;
   d) Estimated as maximum impact level of concerned impacts;
   e) All a, b, c, and d;
   f) Neither a, b, c, nor d.

Q3. Which security problems could be caused by the API abuse?
   a) Directory restriction;
   b) Buffer overflows;
   c) Privacy violation;
   d) Setting manipulation;
   e) All a, b, c, and d;
   f) Neither a, b, c, nor d.

Q4. What are identification requirements?
   a) When application protects itself from infection by unauthorised programs;
   b) When business shall identify its externals before interacting;
   c) When business keeps its sensitive data private from unauthorised use;
   d) When application ensures that its data are not intentionally corrupted;
   e) All a, b, c, and d;
   f) Neither a, b, c, nor d.

Q5. 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 systems should do related to the threats;
   d) They describe what the system should avoid from doing;
   e) All a, b, c, and d;
   f) Neither a, b, c, nor d.
Q6. What is an RBAC role?

a) Any person who interacts with a system;
b) A relationship among sessions;
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.

Q7. Which RBAC functionality should be supported, after user assignments and permission assignments are defined?

a) Transformation of SecureUML diagram to UMLsec;
b) Creation of sessions and checking the access;
c) View of assigned users, roles and their permissions;
d) View session roles and permissions;
e) All a, b, c, and d;
f) Neither a, b, c, nor d.

Q8. What is shoulder surfing?

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

Q9. Which of these “points” do not belong to the “Seven Security Touchpoints”?

a) Maturity of test plans;
b) Security requirements;
c) Risk-based security tests;
d) Penetration testing;
e) All a, b, c, and d do not belong;
f) All a, b, c, and d do belong.

Q10. What is a security criterion?

a) Anything that has value to the organisation
b) A characteristic of an IS asset that can constitute a weakness or a flaw in terms of IS security;
c) A property or constraint on business assets that characterises their security needs;
d) Potential attack, carried out by an agent;
e) All a, b, c, and d;
f) Neither a, b, c, nor d.