SOLUTIONS

(Different solution representations are also possible)

PART I: Internet Store example

Task 1: Fill in Table 1 with the details that correspond to the description of security risk management model.

Table 1. Recognizing concepts of security risk management

<table>
<thead>
<tr>
<th>Concepts of the domain model for the information systems security risk management</th>
<th>What is (are) business asset(s) in the Internet Store example, given Fig. 1, 2, and 3?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assets Business assets</td>
<td>Item list</td>
</tr>
<tr>
<td>Information System assets</td>
<td>Internet store (pool), Accept request for item list (task), Provide (display) item list (task)</td>
</tr>
<tr>
<td>Security criterion</td>
<td>Availability of the item list</td>
</tr>
<tr>
<td>Risk</td>
<td>Violator uses Violator’s profile and executes task “Request item list” for multiple times because number of requests is not limited thus leading to the harm of the task “Provide (display) item list” and negation of availability of the item list.</td>
</tr>
<tr>
<td>Impact</td>
<td>Negates availability of the item list; Harm IS asset – Provide (display) item list Harm business asset – Item list is unavailable</td>
</tr>
<tr>
<td>Event</td>
<td>Violator uses Violator’s profile and executes task “Request item list” for multiple times because number of requests is not limited</td>
</tr>
<tr>
<td>Threat</td>
<td>Violator uses Violator’s profile and executes task “Request item list” for multiple times</td>
</tr>
<tr>
<td>Vulnerability</td>
<td>Number of requests is not limited</td>
</tr>
<tr>
<td>Threat agent</td>
<td>Violator (pool)</td>
</tr>
<tr>
<td>Attack method</td>
<td>Uses Violator’s profile (swimlane), and executes task “Request item list” for multiple times</td>
</tr>
<tr>
<td>Risk treatment decision</td>
<td>Risk reduction</td>
</tr>
<tr>
<td>Security requirements</td>
<td>Check for abnormal request (task) Terminate if not normal</td>
</tr>
<tr>
<td>Controls</td>
<td>Message filtering control</td>
</tr>
</tbody>
</table>
Task 2: If the concept of the security risk management is not represented in the model, define it (and write it in Table 1) following your intuition on the modelled example.

<table>
<thead>
<tr>
<th>Business asset: item list</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impact not explicit:</td>
</tr>
<tr>
<td>• Negates availability of the item list;</td>
</tr>
<tr>
<td>• Harm IS asset – Provide (display) item list</td>
</tr>
<tr>
<td>• Harm business asset – Item list is unavailable</td>
</tr>
<tr>
<td>Risk treatment: risk reduction.</td>
</tr>
<tr>
<td>Control: Message filtering control (firewall).</td>
</tr>
</tbody>
</table>

Task 3: What are the context, assets and their security criteria?
Task 4: How does the security risk constitute itself?

Task 5: What is the countermeasure (i.e., risk treatment, security requirements, and controls), and how does it mitigate the security risk?

Note: Although a picture is worth 1000 words, short textual explanations of the diagrams are welcome!
PART II: Application for Japanese course

Task 6: Using the SecureUML modelling language, create a class diagram, which would define the role-based access control (RBAC) policy.

The class diagram should specify:
- Protected Resource(s), its Attributes and protected Operations
- Users, Roles, and User assignments
Creativity – your key to secure software!!!

- Permissions, Permissions assignment

- Security actions (as separate class diagram)

**Task 7:** Define at least 5 security authorisation constraints.

Plain text constraints are added as comments to the model
Creativity – your key to secure software!!!
BONUS – A Multiple-Choice Questionnaire

[Each correctly answered question gives you 1 point.]

Correct answers are placed in BOLD.

1. What are enterprise security and risk management patterns?
   a) Patterns, which define security constraints at the architectural level, the application level
   b) Patterns, which define specific requirements and design for the identification and authentication services;
   c) Patterns, which are Essential for systems that permit or deny the use explicitly
   d) Patterns, which represent trade-offs between complexity, speed, and security;
   e) All a, b, c, and d;
   f) Neither a, b, c, nor d.

2. What is risk reduction?
   a) An action to lessen the probability, negative consequences, or both, associated with a risk;
   b) A decision not to become involved in, or to withdraw from, a risk;
   c) A decision of how to treat the identified risks;
   d) A sharing with another party the burden of loss from a risk;
   e) All a, b, c, and d;
   f) Neither a, b, c, nor d.

3. Why is consideration of security from early stages of software system development important?
   a) Because it helps envisage threats, their consequences and countermeasures;
   b) Because the need to secure systems and software becomes a necessity rather than an option;
   c) Because it discard design alternatives that do not offer a sufficient security level;
   d) Because it help re-scope or cancel a project if the risk is too high;
   e) All a, b, c, and d;
   f) Neither a, b, c, nor d.

4. What are intrusion detection requirements?
   a) Requirements that characterise the extent to which a business, application, or component shall verify the identity of its externals before interacting;
   b) Requirements that characterise the extent to which an application or component shall ensure that its data and communications are not intentionally corrupted via unauthorized creation, modification, or deletion;
   c) Requirements that characterise the extent to which a business, application, or component shall keep its sensitive data and communications private from unauthorized individuals and programs;
   d) Requirements that characterise the extent to which an application or component shall detect and record attempted access or modification by unauthorized individuals;
   e) All a, b, c, and d;
   f) Neither a, b, c, nor d.
5. What are the problems of input validation and representation?
   a) **Cross-site scripting attacks**;
   b) **Command injection**;
   c) Password management;
   d) **SQL injection**;
   e) All a, b, c, and d;
   f) Neither a, b, c, nor d.

6. What is an access?
   a) A mapping between a user and an activated subset of roles the user is assigned to;
   b) A passive entity that contains or receives information;
   c) **A specific type of interaction between a subject and an object that result in the flow of information from one to the other**;
   d) A job function within the organisation that describes the authority and responsibility conferred on a user assigned to the role;
   e) All a, b, c, and d;
   f) Neither a, b, c, nor d.

7. Which best practices are applied in the comprehensive lightweight application security process?
   a) Institute awareness programs
   b) Perform application assessments
   c) Capture security requirements
   d) Build vulnerability remediation procedures
   e) All a, b, c, and d;
   f) Neither a, b, c, nor d.

8. 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.

9. What is a risk impact?
   a) A component or part of the IS that has value to the organisation and is necessary for achieving its objectives;
   b) A property or constraint on business assets that characterises their security needs;
   c) **A potential negative consequence of a risk that may harm assets of a system or an organisation, when a threat is accomplished**;
   d) A combination of a threat and one or more vulnerabilities
   e) All a, b, c, and d;
   f) Neither a, b, c, nor d.