Introduction

In this course, the written exam will count 50% of the final grade, and the remaining 50% of the final grade comes from the compulsory exercises.

So, your final grade of this course will be:

Points you get from this written exam + points you get from the compulsory exercises.

If you feel that any of the problems require information that you do not find in the text, then you should

- Document the necessary assumptions
- Explain why you need them

Your answers should be brief and to the point.

You need to put all your answers to a .pdf file and upload the .pdf file to Inspera before the examination time expires.

Problem 1 – (32 points in total)

Case description:

Company A hosts a web application that allows users to trade stock shares in Norway.

To use the web application, a user needs to register to fill in the following information.

- User name
- Password
- Personal ID
- Bankaccount number to transfer money from and to this web application
- Contact information including email and mobile phone number

- Home address and postcode
- Upload a copy of the ID card or the first page of the passport

To use the functions of the web application, a user needs to log in using a username and password. A one-time password SMS will be sent to the user's mobile phone as the two-factor authentication.

A "forget password function" is also provided to let the user reset the password. The "forget password function" will send a link in an email to enable the user to reset the password.

By using this web application, the user can:

- See real-time stock share prices
- Buy and sell stock shares
- Transfer money from and to the bank account
- Fill in a web form to send questions to get technical support

By the end of each year, the web application will automatically generate a report that summarizes the balance of the user's account and transaction history and send the report to the National tax office.

You will now work as the security analyzer of this web application. Your task is to make a risk-based assessment of this application based on the RMF (Risk Management Framework).

Your tasks include:

- Task 1: Identify a minimum of 4 business goals, a minimum of 5 business assets, and a minimum of 5 business risks (7 points).

- Task 2: Identify technical risks related to the web application using misuse cases and attack trees (You need to draw at least two misuse cases, three attack trees, and identify at least ten technical risks from the misuse cases and attack trees)
    - Misuse cases and attack trees (5 points)
    - Technical risks (10 points)

- Task 3: Derive security requirements from each technical risk identified, and design and describe black-box penetration test cases (including test steps and expected results of each step) to verify each derived security requirement (10 points)

To present your answers in a structured manner, you may format your solutions like:
Task 1: ...
Task 2: ...
Task 3: ...

Problem 2 – (8 points in total)

Company B is another company that is collaborating with Company A mentioned in problem 1.

Company B provides data analytic services to Company A.

Company B analyzes the transaction data of the users of the web application to understand their trading patterns.

To enable Company B to use the data, Company A must anonymize the users' transaction data to protect their privacy.

The data provided by Company A to Company B are as follows.

ID	Age	Gender	Postcode	Stock share owned	Transaction type	Transaction time stamp	Transaction Amount
1	23	Male	7045	EquiNor	Buy	10.10.19	1000 NOK
2	56	Female	6012	Telenor	Sell	10.08.19	200 NOK
3	40	Female	7322	EquiNor	Sell	04.08.19	4000 NOK
4	33	Male	8401	NEL	Buy	10.10.19	500 NOK
5	70	Male	2100	NEL	Buy	10.08.19	300 NOK
6	33	Female	3400	DNB	Sell	06.10.19	400 NOK
7	45	Male	7049	HYDRO	Buy	01.10.19	2000 NOK
8	46	Female	7001	DNB	Sell	03.03.19	10000 NOK

Suppose you work for Company A. Your task is:

Use the following approach to anonymize the data before sending them to Company B:

- Generalization

- Suppression
- Anatomization
- Permutation

Problem 3 – (5 points in total)

Suppose Company A will deploy the web application to the Microsoft Azure cloud and use the IaaS (Infrastructure as a Service). Based on the content of the "cloud service security lecture," your task is:

Explain to Company A which technical risks you identified in Problem 1 can be mitigated by using particular Microsoft Azure IaaS security features, and which technical risks the Company A developers still need to mitigate themselves.

Problem 4 – (5 points in total)

Company A usually uses the agile development process but has no security focuses on its software development.

Suppose you are a consultant who is going to propose improvements to Company A to improve its software security practices.

Based on the content of the "Agile Security, the BSIMM and OpenSAMM, and any other lectures of this course," your task is:

Propose to Company A possible approaches or strategies it can use to improve the security of its web application. You need to propose at least one approach/strategy in each of the following aspects and explain the benefits of using the approach/strategy.

- Requirements
- Design
- Implementation
- Verification
- Team organization