Kopi av Cover page

Department of (department) Computer Science

Examination paper for (course code) (course title): TDT4237 (Software Security and data privacy) Spring 2022

Examination date: 25.05.2022

Examination time (from-to): 09:00-13:00

Permitted examination support material: All support material is allowed

Academic contact during examination: Jingyue Li
Phone: 9189 7446

Technical support during examination: Orakel support services
Phone: 73 59 16 00

If you experience technical problems during the exam, contact Orakel support services as soon as possible before the examination time expires. If you don’t get through immediately, hold the line until your call is answered.

OTHER INFORMATION

Do not open Inspera in multiple tabs, or log in on multiple devices, simultaneously. This may lead to errors in saving/submitting your answer.

Get an overview of the question set before you start answering the questions.

Read the questions carefully, make your own assumptions and specify them in your answer. Only contact academic contact if you think there are errors or insufficiencies in the question set.

Make your own assumptions: If a question is unclear/vague, make your own assumptions and specify them in your answer. Only contact academic contact in case of errors or insufficiencies in the question set.

Cheating/Plagiarism: The exam is an individual, independent work. Examination aids are permitted, but make sure you follow any instructions regarding citations. During the exam it is not permitted to communicate with others about the exam questions, or distribute drafts for solutions. Such communication is regarded as cheating. All submitted answers will be subject to plagiarism control. *Read more about cheating and plagiarism here.*

Notifications: If there is a need to send a message to the candidates during the exam (e.g. if there is an error in the question set), this will be done by sending a notification in Inspera. A dialogue box will appear. You can re-read the notification by clicking the bell icon in the top right-hand corner of the screen. All candidates will also receive an SMS to ensure that nobody misses out on important information. Please keep your phone available during the exam.

Weighting: 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.

The weight of each question is on the question. For **Closed Ended questions (1 point for each question if the answer is correct, 0 point if the answer is wrong).**

ABOUT SUBMISSION

Answering in Inspera: If the question set contains questions that are not upload assignment, you must answer them directly in Inspera. In Inspera, your answers are saved automatically every 15 seconds.

NB! We advise against pasting content from other programs, as this may cause loss of formatting and/or entire elements (e.g. images, tables).

File upload: When working in other programs because parts of/the entire answer should be uploaded as a file attachment – make sure to save your work regularly.

All files must be uploaded before the examination time expires.

The file types allowed are specified in the upload assignment(s). Note that it is only possible to upload one file per upload assignment.

30 minutes are added to the examination time to manage the sketches/calculations/files. The additional time is included in the remaining examination time shown in the top left-hand corner.

NB! You are responsible to ensure that the file(s) are correct and not corrupt/damaged. Check the file(s) you have uploaded by clicking "Download" when viewing the question. All files can be removed or replaced as long as the test is open.

How to digitize your sketches/calculations
How to create PDF documents
Remove personal information from the file(s) you want to upload

Automatic submission: Your answer will be submitted automatically when the examination time expires and the test closes, as long as you have answered at least one question. This will happen even if you do not click "Submit and return to dashboard" on the last page of the question set. You can reopen and edit your answer as long as the test is open. If no questions are answered by the time the examination time expires, your answer will not be submitted. This is considered as "did not attend the exam".

Withdrawing from the exam: If you become ill during the exam or wish to submit a blank answer/withdraw from the exam for another reason, go to the menu in the top right-hand corner and click "Submit blank". This cannot be undone, even if the test is still open.

Accessing your answer post-submission: You will find your answer in Archive when the examination time has expired.

1 Part 1 tasks

See the attached PDF for case and tasks descriptions. Upload your answers in a PDF below.

Last opp filen her. Maks én fil.

Alle filtyper er tillatt. Maksimal filstørrelse er **50 GB**.

Velg fil for opplasting

Maks poeng: 25

2 Confidentiality, Integrity and Availability (3 points)

Within your organization, you as an admin of the servers, have a server called Server1 that is running Window Server 2008. On Server 1, you create and share a folder called Data on the C drive. Within the Data folder, you create a folder for each user within your organization. You then place each person's electronic paycheck in his or her folder. Later, you find out that John was able to go in and change some of the electronic paychecks and delete others. Explain which of the Confidentiality, Integrity and Availability components was not followed in this scenario.

Skriv ditt svar her

Format

Words: 0

Maks poeng: 3

3 Changing Passwords (3 points)

Imagine that you work for CCorp. Your CIO tells you that he just got a message on his computer saying that he has to change his password. He asks you to make an exception to him in the rules so he does not need to change the password often and also that he could have a shorter password. What will you answer, and how will you justify your answer?

Skriv ditt svar her

Format

Words: 0

Maks poeng: 3

4 Exposure of Sensitive Information (3 points)

List 3 examples of vulnerabilities that can expose sensitive information and explain briefly how the vulnerabilities could be exploited.

Skriv ditt svar her

Format

Words: 0

Maks poeng: 3

5 Vulnerable and Outdated Components (3 points)

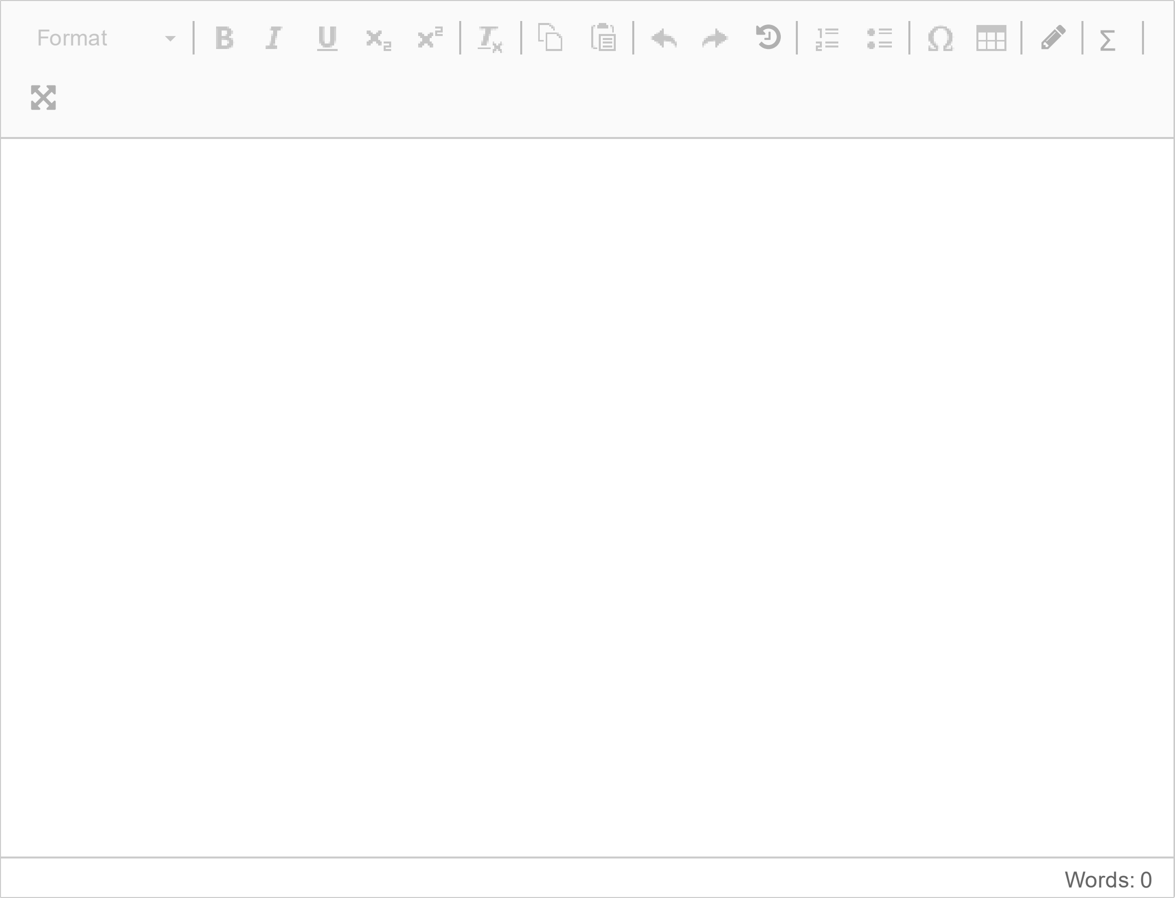
Imagine you are the security engineer in one software team. And the team run some analysis tools and find out that 5 components have vulnerabilities.

Component 1: CVSS Score Low (3,5) and very much used component in the system
Component 2: CVSS Score Medium (5,5) very much used component in the system
Component 3: CVSS Score High (7,5) not so much used component in the system
Component 4: CVSS Score High (8,0) and very much used component in the system
Component 5: CVSS Score Critical (9,5) not so much used component in the system

The team then ask you what should they do with the vulnerable components, fix right away, wait more time, do nothing, stop development to fix the vulnerabilities.

Which types of further details would you ask the team about the components and the vulnerabilities? How could you use CVSS metrics to answer this question?

Skriv ditt svar her



Maks poeng: 3

6 Web Security (3 points)

You are visiting a (not very professional) Web shop. In the address bar of your browser you see the following URL (do not try the link):

```
http://bestwebshop.com/?page=index.html
```

From that you can derive two (2) security issues/vulnerabilities for this Web page. Please describe them.

Skriv ditt svar her

Format

Words: 0

Maks poeng: 3

7 Which of following most accurately describe the purposes of CVE and CVSS?

Velg ett alternativ:

○ CVSS provides a score that indicates the severity of a vulnerability. CVE is a list of publicly known vulnerabilities containing ID numbers, descriptions, and references.

○ CVSS is a “low and slow” style of attack executed to infiltrate a network and remain inside undetected. CVE is a list of publicly known vulnerabilities containing ID numbers, descriptions, and references.

○ CVSS provides a score that indicates the severity of a vulnerability. CVE integrates all the security tools available in an organization and automates incident responses.

○ CVSS provides a list of top vulnerabilities. CVE is a list of scores for vulnerabilities in a system.

Maks poeng: 1

8 In an asymmetric key system, each user has a pair of keys: a private key and a public key. To send an encrypted message to someone, what must you encrypt the message with?

Velg ett alternativ:

○ The recipient’s public key

○ Your public key

○ Your private key

○ The recipient’s private key

Maks poeng: 1

9 OmniTec’s new programmer has left several entry points in its new e-commerce shopping cart program for testing and development. Which of the following terms best describes these entry points?

Velg ett alternativ:

○ SQL injections

○ XSS

○ Trojan

○ Backdoor

Maks poeng: 1

10 When the cost of a countermeasure outweighs the value of the asset, which of the following is the best approach?

Velg ett alternativ:

○ Increase the value of the asset

○ Increase the cost of exposure

○ Take no action

○ Mitigate the risk

Maks poeng: 1

11 Phishing Attacks

Several of your organization’s employees have been hit with email scams over the past several weeks. One of these attacks successfully tricked an employee into revealing his username and password. Management has asked you to look for possible solutions to these attacks. Which of the following is the best solution?

Velg ett alternativ:

○ Increase the organization’s email-filtering ability.

○ Implement a new, more robust password policy that requires complex passwords.

○ Develop a policy that restricts email to official use only.

○ Start a training and awareness program.

Maks poeng: 1

12 Taboo trap

What is the purpose of a "Taboo trap" in machine learning?

Velg ett alternativ:

○ Predict illegal social behaviour patterns

○ Detect adversarial input

○ Deliberately adding illegal input to the training data to make the model more robust

○ Checking for classifications that are ethically wrong

Maks poeng: 1

13 What is considered as lawful consent in the GDPR?

Velg ett alternativ:

○ A continuation of navigation on a site of a mobile application by a simple scroll.

○ A clear affirmative act by which the person freely expresses, in a specific and informed manner, their consent to data processing.

○ None of the alternatives

○ The simple act of downloading a document from a site or a mobile application.

Maks poeng: 1

14 After Debbie becomes the programmer for the new payroll application, she places some extra code in the application that will cause the program to halt if she is fired and her name is removed from payroll. What type of attack can be launched?

Velg ett alternativ:

○ Buffer overflow

○ Logic bomb

○ Salami attack

○ Rounding down

Maks poeng: 1

15 Unicode games

How can you sabotage an automatic translation system using unicode characters?
Velg ett alternativ:

○ Replace a character with a symbol that looks like the regular character

○ Add characters that are longer than the allowed input buffer

○ Switch from UTF-8 to ISO 8859-1 encoding

○ Poison the traning data with illegal unicode characters

Maks poeng: 1

16 Which of the following is a disadvantage of symmetric encryption compared to asymmetric encryption?

Velg ett alternativ:

○ Key size

○ Key strength

○ Key management

○ Speed

Maks poeng: 1

17 Code to setup password policy (4 points)

Suppose the password policy of a system is as follows.

The password should be as long as possible and must contain at least 10 characters.

The passwords have to contain at least one character from the following four groups:

- **Upper-case letters: A–Z**
- **Lower-case letters: a–z**
- **Numbers: 0–9**
- **The following special characters: !#()+,.=?@[]_{}-**

Spaces and the letters "æ", "ø" and "å" are not accepted

Your task is to develop code and configure Password Validators in Django to check the policy.
Please add your code and explanation below.

Skriv ditt svar her

Maks poeng: 4

18 Insufficient logging and monitoring vulnerability (2 points)

```
LOGGING = {
    'version': 1,
    # Version of logging
    'disable_existing_loggers': False,
    #disable logging
    # Handlers #############################################################
    'handlers': {
        'file': {
            'level': 'WARNING',
            'class': 'logging.FileHandler',
            'filename': 'dataflair-debug.log',
        },
########################################################################
        'console': {
            'class': 'logging.StreamHandler',
        },
    },
    # Loggers ####################################################################
    'loggers': {
        'django': {
            'handlers': ['file', 'console'],
            'level': 'LOGLEVEL',
        },
    },
}
```

The above code has insufficient security logging and monitoring vulnerability. Please propose one solution (by updating the code) to fix the vulnerability.

Skriv ditt svar her

Maks poeng: 2

Question 1

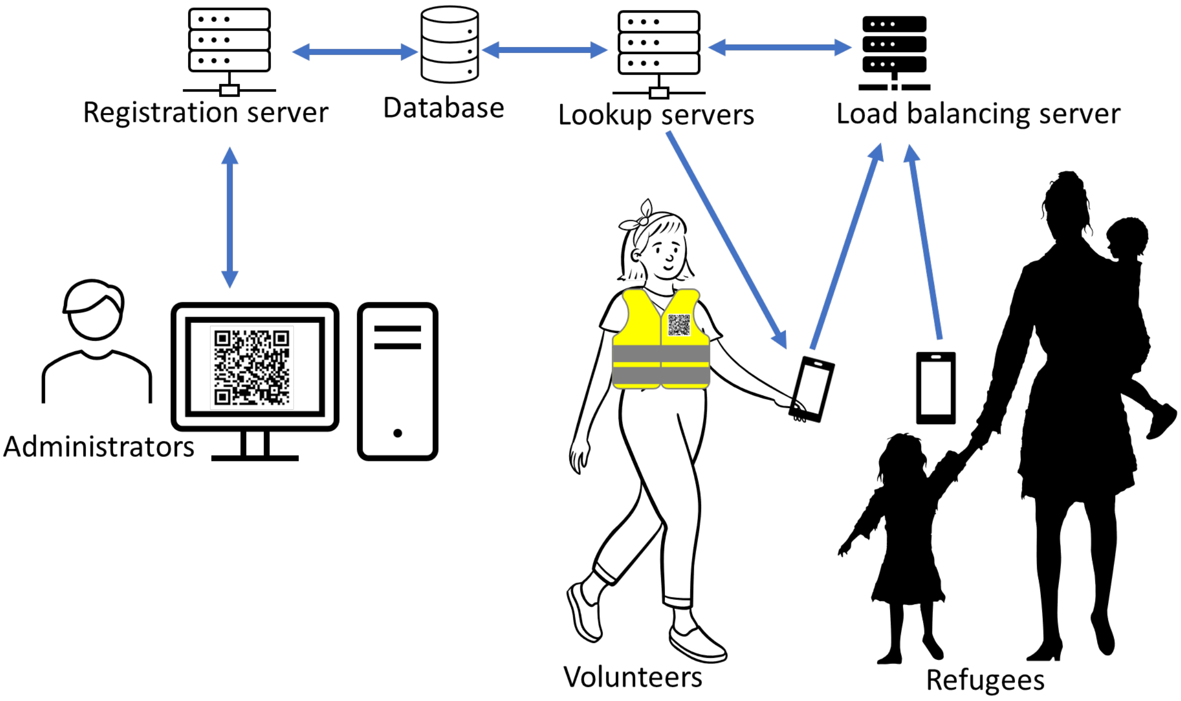
Attached

Part 1 Case description:

During a crisis, refugees arrive from a conflict area to neighbouring countries and are in need of shelter, food and a safe environment. At the refugee camps, there are many volunteers working to provide different types of support services and perform various tasks, such as medical personnel, truck drivers, cooks, observers, journalists and administrators. These people are organised in a relatively flat structure and come in from all over Europe. It is currently a challenge to identify people and verify their roles. Also, the refugees need to be assured that the volunteers are who they claim to be and can be trusted. There are already known incidents of robbery and trafficking.

You are part of a team that has been asked to develop a system for keeping track of volunteers. The same system will also be used to register refugees as they arrive. You can assume that all people involved have access to mobile phones with cameras and a relatively stable Internet connection. The administrators of the camps need a Web-based interface to register people. Once registered, QR-codes will be printed on vests, bracelets and ID-cards, which anyone can quickly scan using their phone. The QR-codes should be used to lookup and retrieve information online, such as ID number, picture, name, nationality, role and spoken languages. For refugees, there might also be personal data about medical condition and family members.

The figure below shows a rough sketch of the system. An SQL database is used both by the Registration server and the Lookup servers. A load balancing server distributes incoming traffic to the Lookup servers. You have approximately one week to develop and deploy. You can make further assumptions on the situation, and you also need to assume that there are threat agents present.



Part 1 tasks (25 points in total)

In this part you will do a risk-based assessment based on RMF (Risk Management Framework) of the system described in the case.

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

- Document the necessary assumptions (e.g. technology, standards, software, design choices.)
- Explain why you need them

Your answers should be brief and to the point. You need to put all your answers in a .pdf file and upload the .pdf file to Inspera before the examination time expires.

Task 1. Identify business goals (at least 5) and business assets (at least 5). (4 points)

Task 2. Identify business risks (at least 5) and define relevant risk dimensions and scales. Hints: Likelihood could be based on expected frequency or could be attacker-centric. One of the impact dimensions should be related to privacy. (4 points)

Task 3. Create an overall misuse case diagram for the system described in the case, which should contain at least 5 threat agents/actors. Justify and rank the threat agents in a separate table according to your own criteria. (3 points)

Task 4. From your misuse case diagram, select at least one misuse case activity and create a corresponding attack tree. (2 points)

Task 5. Based on your threat models (misuse case and attack tree(s)), identify at least 10 technical risks. You should describe necessary assumption related to the technology. Link these to the business risks and make a justified ranking of them. Show the business risks in a risk matrix. (4 points)

Task 6. Select at least 3 technical risks and define security requirements for each as part of a risk mitigation strategy. (2 points)

Task 7. This system will be operated by a non-profit organisation of volunteers, with no real financial turnover. Write a short discussion about potential GDPR violations based on the privacy principles (art.5). Mention dilemmas of applying GDPR in times of crises. (3 points)

Task 8. In a future version of the system, there is a possibility that machine learning will be used to confirm the identities of the users. Write a short discussion on how machine learning techniques could be used and misused/fooled in this context. Give examples for both cases. (3 points)