Høyskolen Kristiania

Emnekode:	**TK2100 – eksamen (Bergen)**
Emnenavn:	**Informasjonssikkerhet**
Vurderingskombinasjon:	**24 timer hjemmeeksamen**
Vurderingsform:	**Bestått / ikke bestått**
Innleveringsdato:	**29. april 2025**
Filformat:	**PDF**

The question set consists of 4 pages and contains a total of 10 questions to be answered. (Exam should be answered in English.)

There is a 24-hour deadline for this home exam, but the expected workload is 4-6 hours, so it is not the intention to "work through the night". Please note that the exam MUST be submitted by the deadline set, and must be submitted via the exam platform WISEFLOW. It will not be possible to submit the assignment after the deadline – this means that you should submit well in advance so that you can contact the exam office or user support if you have technical problems.

As this is a home exam, it is important to show an understanding of the topics, and the assignments have a greater degree of debate and analysis. Supplementary and explanatory answers are therefore expected to all assignments. You can choose to draw figures and sketches in the word processor, or by drawing on paper and uploading an image – remember to insert the image in the correct place in the answer. (Pictures that are attached but not included in the paper are not considered part of the submitted exam paper.)

It is specified that the student must answer the exam independently and individually, collaboration between students and plagiarism is not allowed. All use of text, images and illustrations that are taken from lectures, textbooks or the internet must be recorded with source references so that it is clear what is the student's own work, the APA7 standard is recommended to be used for sources. For the top score on questions, the answers should be supported by relevant sources in addition to ordinary syllabus literature. (Please note that copying text from your own previous submitted assignment/exam may be considered "self-plagiarism" if you do not cite yourself correctly as the source.)

It is also clarified that according to the school's exam regulations, it is not allowed to present someone else's work as your own – this includes work done by artificial intelligence (such as text or code generation models).

The answer should not be more than 15 A4 pages, with font size 12, normal margins and line spacing 1.0.

Task 1. General (10 %)

Define "information security". Use the CIA model as a basis for your answer.

Task 2. Surveillance (10 %)

Discuss how national authorities can use your network traffic to map you as a private individual, and your movements and actions. Discuss how “Etterretningstjenesteloven”, Chapter 7 may affect private individuals in Norway.

Familiarize yourself with the term "chilling effect" used in this context, and discuss ethical issues related to this type of surveillance.

Task 3. Malware (10 %)

Explain the difference between a virus and a worm. You should refer to at least one example of each of these two types of malware and explain how they spread.

Task 4. Encryption (10 %)

Explain how data can be signed with asymmetric encryption, provide at least one example of an algorithm that can do this, and explain how this algorithm works when used for signing.

Explain conceptually how a document can be digitally signed in this way, explain which parts of the CIA model this safeguards and discuss whether other security requirements are also met by this.

Task 5. Personal Security (10 %)

Explain 5 technical steps you can take to strengthen your personal security within the digital domain (these can be steps you have already taken). Explain what problems each of these steps solves and why this is important to you.

Task 6. Web security (10 %)

Explain how Cross Site Request Forgery works, and what distinguishes this attack from other web-based attacks. Discuss specific areas of use for CSRF attacks, and how to defend against such attacks.

Husk å oppgi kandidatnummer på din besvarelse, ikke studentnummer.

Task 7. Network (10 %)

Explain what security challenges we have at the link layer in the TCP/IP model.

Task 8. Home office (10 %)

During the COVID pandemic, it became common to work from home for most companies and employees with typical "office work". Discuss the challenges this poses to information security in the companies. What do you think needs to change to ensure security now that working from home has become the "new norm" in many companies?

Task 9. Practical anti-virus (10 %)

In this assignment, you will demonstrate your knowledge of using anti-virus software. Download the EICAR test file from https://www.eicar.org/download-anti-malware-testfile/. You can either download one of the files or you can create a new file with the 68 characters that make up the "virus's" signature as described at the bottom of the page (and as used in the lab exercises). You must further demonstrate the following:

1. Scan the file with your anti-virus program, show that the anti-virus program detects the file and report it as malware
2. Go into your anti-virus program's quarantine function, find the detected file and export it out of quarantine (for some anti-virus programs you may need to turn off real-time protection first)

Document the two steps with screenshots from your anti-virus program, explaining what you are doing and why.

If you (despite what you have learned in this course) do not have anti-virus software on your computer, you will need to install it for this task.

Task 10. Simulation of Attack (10 %)

You need to answer only one of the two tasks, i.e., choose either (a) or (b).

(a) Practical server-side attack

In this exercise, you will use the web application "Boris Lockpicks" that you installed in the practice lessons for lesson 8 Web Security. Demonstrate against this web application how to perform a "local file inclusion" attack.

Simulate the attack by printing the contents of the file 'backend/sendemail.c' on the screen. Document with screenshots and explain your procedure. Remember to insert the screenshot in the correct place in the answer.

(b) Practical cross-site scripting attack

Demonstrate an XSS attack against a web application using Google XSS Game.

Simulate the attack by triggering a popup box on the screen using JavaScript that displays the text:

"Student Id XXXX", where XXXX is your candidate number for this exam.

Document your process clearly with screenshots and explain each step of your method. Remember to place your screenshots in the correct locations within your answer.

Link to the Google XSS Game: https://xss-game.appspot.com/

End of the question set