JÖNKÖPING UNIVERSITY
School of Engineering

Study guide
Information Security
7,5 ECTS

Course name:	Information Security
Ladok code:	TIAN19, TIHG10
Credits:	7,5
Year:	2020
Course coordinator:	Erik Bergström
Examiner:	Sonny Johansson

1 TEACHERS

Erik Bergström

Course coordinator, lecturer

Contact details

- E-mail: erik.bergstrom@ju.se
- Phone:036 - 550 24 20

Sonny Johansson

Examiner

Contact details

- E-mail: sonny.johansson@ju.se
- Phone:036 - 10 15 76

2 INTRODUCTION

In today's society, there are high requirements for information security. The course aims at giving an overview of the information security domain by introducing basic concepts, principles, models, and standards. The course also includes human factors in the security process and the human's role in the information security domain. The field is interdisciplinary with connections to other fields such as, e.g., law, and ethics which is also included in the course. The course includes the following elements:

- Basic concepts within information security
- Authentication methods
- Malware and malicious software
- Operating systems security
- Network security
- Information security management
- Physical security
- Current events and trends within information security

3 INTENDED LEARNING OUTCOMES

The intended learning outcomes of the course are found and are described under the next heading.

4 EXAMINATION, ILOS AND LEARNING ACTIVITIES

4.1 DESCRIPTION OF THE ELEMENTS THAT EXAMINE THE COURSE ILOS, AND THE CORRESPONDING LEARNING ACTIVITIES

Intended learning outcomes	Examined elements	Learning activities
Display knowledge of basic concepts, principles, laws, models, and standards within the area of information security	Written examination	Lectures
Display knowledge of recent cases of data breaches and/or information leakage, and show an understanding of the underlying reasons	Written examination, seminar	Lectures, seminars
Display knowledge of how information security is practiced in an organization	Written examination	Lectures
Display knowledge of technical and administrative security mechanisms	Written examination	Lectures
Demonstrate the ability to search for and present relevant research results related to current events and/or trends within the field of information security	Seminar	Lectures, seminars
Demonstrate the ability to analyze and reflect over current events and/or trends within the area of information security	Seminar	Lectures, seminars
Demonstrate the ability to reflect over how vulnerabilities in information systems affect organizations and society	Written examination, seminar	Lectures, seminars

4.2 INFORMATION TO STUDENTS

To achieve the learning objectives in the course, you should attend and actively participate in the seminars and lectures offered in the class. Active participation means, among other things, that you ask questions when there is something you do not understand or want to be explained in another way. If you feel that you have not received the support you expected, you should contact the course coordinator.

4.3 CONDITIONS FOR THE EXAMINED ELEMENTS

Written examination: The written examination comprises 5 credits and determines the grade of the course ("5", "4", "3", or "fail"). The written examination is conducted after the course has ended at the beginning of December. The primary aim of the written examination is to assess the achievement of the learning outcomes addressed in the lectures. Don't forget to register at least ten days in advance. The course coordinator will visit the exam to answer any questions. The re-examination is scheduled according to the academic year's planning.

Seminars: The examination "seminars" comprises 2.5 credits. The seminar part is graded pass or fail. To receive a passing grade, the following three parts should be graded with a Pass: (1) Seminar 1: summary graded as pass and active participation in the seminar is required, (2) Seminar 2: report graded as pass and active participation in the seminar is required, and (3) Seminar 3: report graded as pass and participation in the presentation required.

4.4 RE-EXAMINATION OF THIS COURSE

The same criteria are used for the re-examination of the course.

5 GRADING CRITERIA

Examined elements	Grading criteria grade 3/Pass[2]	Grading criteria grade 4	Grading criteria grade 5
Written examination[1]	>=50%	>= 70%	>=85%
Seminars	Pass[3]		

[1] Determines the final grade of the course, which is issued when all course units have been passed.

[2] It is possible to obtain up to 6% by passing three quizzes (3*1p). These points count towards getting the grade 3/Pass. The points do not count towards achieving a higher grade than 3, and only for the first exam (not re-exams).

[3] To obtain the grade Pass, the three parts described in section 4.3 should be graded with a Pass.

6 COURSE LITERATURE AND OTHER TEACHING AIDS

The lectures are primarily based on Pfleeger, Pfleeger, and Margulies (2015). The exact reading instructions (i.e., which chapters to read) are available below.

The book by Pfleeger, Pfleeger, and Margulies (2015) is available as a physical book (ISBN 9780134085043), and as an e-book (ISBN: 9780134085050).

Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2015). Security in Computing (Fifth ed.): Prentice Hall.

7 TIME PLAN

Purple = deadline examined element
Green = quizzes

Date	Teacher/guest	Learning activities	Course literature
Week 43	Erik Bergström	Module 1 - Course introduction	Chapter 1 – Introduction
Week 43	Erik Bergström	Module 2 – Authentication and access control	Chapter 2.1 - Authentication Chapter 2.2 – Access control
Week 44	Erik Bergström	Module 3 – Privacy, legal issues, and ethics	Chapter 9 - Light Chapter 11 - Light
Week 44	Erik Bergström	Module 4 – Programs and programming	Chapter 3.1 - Unintentional (nonmalicious) programming oversights (light) Chapter 3.2 – Malicious code Chapter 3.3 – Countermeasures (199-216 light)
Week 44	Erik Bergström	Supervision	

Week 45	Erik Bergström	Quiz 1	Monday 09.30-09.40 (Module 1-2)
Week 45	Erik Bergström	Module 5 – Web security	Chapter 4
Week 45	Erik Bergström	Supervision	
Week 45	**Seminar 1, and hand in the summary**		
Week 46	Erik Bergström	Module 6 – Operating systems	Chapter 5.1 - Security in operating systems (not 298-308) Chapter 5.2 - Security in the design of operating systems (316-329 light) Chapter 5.3 - Rootkit (light)
Week 46	Erik Bergström	Supervision	
Week 46	Erik Bergström	Module 7 – Network security	Chapter 6.1 – Network concepts Chapter 6.2 - Threats to network communications Chapter 6.3 – Wireless network security (WEP is light) Chapter 6.4 - Denial-of-service Chapter 6.5 - Distributed denial-of-service Chapter 6.6 - Cryptography in network security Chapter 6.7 - Firewalls Chapter 6.8 - Intrusion detection and prevention systems Chapter 6.9 – Network management
Week 47	Erik Bergström	Module 8 – Management	Chapter 10 – Management and incidents
Week 47	Erik Bergström	Supervision / Mandatory check with supervisor / Registration in Canvas	
Week 47	Erik Bergström	Quiz 2	Monday 09.30-09.40 (Module 3-6)
Week 48	Håkan Sonesson	Guest lecture	Information security management in practice
Week 48	**Seminar 2, and hand in the report**		
Week 48	Erik Bergström	Module 9 - Cryptography	Chapter 2.3 Chapter 12 – Light (except 768-774, 777-788, and 799-802)
Week 49	Erik Bergström	Supervision	
Week 49	Erik Bergström	Quiz 3	Monday 09.30-09.40 (Module 7-9)
Week 50	**Seminar 3, presentation, and hand in the report**		
Week 51	**Written examination (16/12)**		

JÖNKÖPING UNIVERSITY

School of Engineering