

Recent announcements



Announcements shown on the top of Home

(https://canvas.kth.se/courses/64038/discussion_topics/517017)

To add one or more announcements on the homepage, the course responsible or teacher can click: Settings Course details more options mark "Show recent announcements on course home page". Edit the "Number of announcements shown on the homepage" to your preference.

← [Reply](#)

(https://canvas.kth.se/courses/64038/discussion_topics/517017)

Posted on:

Welcome to Computer Security, Cybersecurity Overview, and Cybersecurity Project (<https://canvas.kth.se/courses/64038/pages/general-information>)

Office hours: TBA

Queue for labs: <https://queue.csc.kth.se/Queue/Dasak> (<https://queue.csc.kth.se/Queue/Dasak>)

Course email address: security-dd239x@kth.se (<mailto:security-dd239x@kth.se>)

News Corner

- Friday 24/7/2026: Check out [Frequently Asked Questions \(https://canvas.kth.se/courses/64038/pages/frequently-asked-questions-faq\)](https://canvas.kth.se/courses/64038/pages/frequently-asked-questions-faq) of the course

Course Instructors and TAs

Course responsible and examiner (DD2395/DD2391 Computer Security/Cybersecurity Overview) : [Musard Balliu \(https://www.csc.kth.se/~musard/\)](https://www.csc.kth.se/~musard/) ([musard@kth.se \(mailto:musard@kth.se\)](mailto:musard@kth.se))

Course responsible and examiner (DD2394 Cybersecurity Project): [Roberto Guanciale \(https://www.csc.kth.se/~robertog/\)](https://www.csc.kth.se/~robertog/) ([robertog@kth.se \(mailto:robertog@kth.se\)](mailto:robertog@kth.se))

Teachers: [Musard Balliu \(https://people.kth.se/~musard/\)](https://people.kth.se/~musard/) ([musard@kth.se \(mailto:musard@kth.se\)](mailto:musard@kth.se)), [Sonja Buchegger \(https://www.csc.kth.se/~buc/\)](https://www.csc.kth.se/~buc/) ([buc@kth.se \(mailto:buc@kth.se\)](mailto:buc@kth.se)), [Roberto Guanciale \(https://www.csc.kth.se/~robertog/\)](https://www.csc.kth.se/~robertog/) ([robertog@kth.se \(mailto:robertog@kth.se\)](mailto:robertog@kth.se))

Teaching Assistants: [Eric Cornelissen \(https://www.kth.se/profile/ericco\)](https://www.kth.se/profile/ericco), [Frank Reyes García \(https://www.kth.se/profile/frankrg\)](https://www.kth.se/profile/frankrg), Ziyuan Jia, [SiKai Lu \(https://www.kth.se/profile/sikai\)](https://www.kth.se/profile/sikai), [Mojtaba Moazen \(https://www.kth.se/profile/moazen/\)](https://www.kth.se/profile/moazen/), [Antonio Napoli \(https://www.kth.se/profile/anapoli\)](https://www.kth.se/profile/anapoli), [Tom Sorger \(https://www.kth.se/profile/sorger\)](https://www.kth.se/profile/sorger)

Course Representatives: TBA

Quick Links

- The complete schedule for course activities (lectures, labs, seminars) can be found [here \(https://www.kth.se/social/course/DD2395/calendar/\)](https://www.kth.se/social/course/DD2395/calendar/).
- Frequently Asked Questions (FAQs) can be found [here \(https://canvas.kth.se/courses/64038/pages/frequently-asked-questions-faq\)](https://canvas.kth.se/courses/64038/pages/frequently-asked-questions-faq).
- Information about lab assignments, exercises, seminar, and more can be found [here \(https://canvas.kth.se/courses/64038/assignments\)](https://canvas.kth.se/courses/64038/assignments).
- Information about the [\(https://canvas.kth.se/courses/64038/pages/information-about-projects\)](https://canvas.kth.se/courses/64038/pages/information-about-projects) seminar can be found [here \(https://canvas.kth.se/courses/64038/assignments/385122\)](https://canvas.kth.se/courses/64038/assignments/385122).
- Information about the project can be found [here \(https://canvas.kth.se/courses/64038/assignments/385117\)](https://canvas.kth.se/courses/64038/assignments/385117).
- Past exams and solutions can be found [here \(https://canvas.kth.se/courses/64038/pages/past-exams\)](https://canvas.kth.se/courses/64038/pages/past-exams). Note that the structure and content of the written exam may change in line with the course program of this year.

Course Literature

This course does not use a specific book. Teaching material consists of handouts, papers, and other material distributed by the teachers. For complementary reading on the subject, we recommend the following books:

- [Security Engineering, Ross Anderson, 3rd edition](https://kth-primo.hosted.exlibrisgroup.com/permalink/f/b27hfs/46KTH_ALMA_DS51188515090002456)  (https://kth-primo.hosted.exlibrisgroup.com/permalink/f/b27hfs/46KTH_ALMA_DS51188515090002456)
- [Computer Security, Dieter Gollmann](https://ebookcentral-proquest-com.focus.lib.kth.se/lib/kth/detail.action?docID=819182) (<https://ebookcentral-proquest-com.focus.lib.kth.se/lib/kth/detail.action?docID=819182>)

(Tentative) Course Schedule

When/Where	Topic	Preparation/Reading Material
August 27, 15:00-17	Course overview, introduction to computer security (Slides)	• Introduction to cybersecurity (https://canvas.kth.se/courses/64038/files/10454978?wrap=1)  (https://canvas.kth.se/courses/64038/files/10454978/download?download_frd=1) (F. B. Schneider) • Security principles, Section 1 (https://canvas.kth.se/courses/64038/files/10454965?wrap=1)  (https://canvas.kth.se/courses/64038/files/10454965/download?download_frd=1) (J. Saltzer & M. Schroeder)
August 28, 10:00-12	Cryptography 101 (Slides)	• Cryptography (https://textbook.cs161.org/crypto/), Chapter 5, 6 (Wagner et al.)
August 31, 8:00-10	Roberto presents project task for DD2394 and DD2391	• Only students that read DD2394 and DD2391 should attend
August 31, 13:00-15	Cryptography 101 (Slides)	• Cryptography (https://textbook.cs161.org/crypto/), Chapter 7, 8, 9, 11, 12 (Wagner et al.)
September 1, 8:00-10	Authentication and Authorization (Slides)	• Authentication for people, Section 5.1 (https://canvas.kth.se/courses/64038/files/10454968?wrap=1)  (https://canvas.kth.se/courses/64038/files/10454968/download?download_frd=1) (F. B. Schneider), Passwords, Chapter 14  (https://textbook.cs161.org/crypto/passwords.html) (Wagner et al.) • Discretionary Access Control (https://canvas.kth.se/courses/64038/files/10454984?wrap=1)  (https://canvas.kth.se/courses/64038/files/10454984/download?download_frd=1) , Section 7.1

		(expect 7.1.3), 7.2, 7.4 (F. B. Schneider) • Mandatory Access Control (https://canvas.kth.se/courses/64038/files/10455002?wrap=1)  (https://canvas.kth.se/courses/64038/files/10455002/download?download_frd=1) , Section 8.1 (F. B. Schneider)
September 7, 15:00-17	Cryptography 2 (Slides)	• Interactive AES  (https://formaestudio.com/rijndaelinspector/archivos/Rijndael_Animation_v4_eng-html5.html). • Cryptography (https://textbook.cs161.org/crypto/), Chapter 6, 10, 11 (Wagner et al.)
September 8, 8:00-10	Web Application Security (Slides)	• Web Security  (https://textbook.cs161.org/web/) Chapter 17-22 (Wagner et al.)
September 15, 10:00-12	Security protocols (Slides)	• TLS  (https://textbook.cs161.org/network/) Chapter 31 (Wagner et al.)
Prerequisite for the next 4 lectures	We have prepared some pedagogical material on malware. We advice to look at this material before the lectures below. (Slides, Videos  (https://www.youtube.com/playlist?list=PLiLnGI3H8lm02yzdpU6sShQn0AzwPCALD), Video on Stuxnet  (https://www.youtube.com/watch?v=XGy3cvbYhzQ).	• Malware  (https://textbook.cs161.org/network/malware.html) Chapter 38 (Wagner et al.)
September 15, 15:00-17	Denial of Service vulnerabilities, Firewalls and intrusion detection systems (Slides)	
September 21, 8:00-10	Memory safety (Slides)	• Memory safety (https://textbook.cs161.org/memory-safety/) Chapters 2 and 3 (Wagner et al.) • Code injection in Super Mario world ◦ Slides (https://canvas.kth.se/courses/49134/files/8331330?wrap=1) (https://canvas.kth.se/courses/49134/files/8331330/download?

		download_frd=1) ◦ Video 1 (https://www.youtube.com/watch?v=TqK-2jUQBUY) (https://www.youtube.com/watch?v=hB6eY73sLV0) ◦ Video 2 (https://www.youtube.com/watch?v=hB6eY73sLV0)
September 22, 10:00-12	System security (Slides)	• Memory safety (https://textbook.cs161.org/memory-safety/) Chapters 4 (Wagner et al.) • Chapter 10 Isolation: Mapping and Multiplexing (F. B. Schneider) (F. B. Schneider)  (https://www.cs.cornell.edu/fbs/publications/chptr.isolate.sysConstructs.pdf)
September 28, 10:00-12	Side channels (Slides)	• AES example  (https://eprint.iacr.org/2005/271.pdf) • Chapter 13 Unexpected Communications Channels (F. B. Schneider)  (https://www.cs.cornell.edu/fbs/publications/chptr.chnls.pdf)
September 28, 13:00-15	Spectre and HW security (Slides)	• Spectre  (https://dl.acm.org/doi/abs/10.1145/3399742)
October 5, 10:00-12	Exam preparation (Slides)	
October 6, 10:00-12	Social engineering and exam preparation for that (Slides)	
October 19, 14:00-18	Written exam	
December 16, 14:00-18	Written re-exam	

Please note that all activities below are mandatory to pass the course (unless stated otherwise or you are taking DD2394)

Labs

The course has **3 mandatory lab assignments**, 2 of which are carried out individually and one in groups of 3 students, and an optional lab assignment. The assignments are graded Pass/Fail and a student should pass all assignments (in addition to other requirements) in order to

pass the LAB part of the course. Find below the list of lab assignments, which will appear under [Assignments](https://canvas.kth.se/courses/64038/assignments) (<https://canvas.kth.se/courses/64038/assignments>) in due time.

- Lab G (Secure email with GPG): This lab is done **individually** and is **graded automatically** by the submission system.
- Lab W (Web application security): This lab is done in **groups of 3 students** and **requires a presentation of solutions** to TAs during pre-scheduled lab sessions. By solving additional tasks, you can earn 1 merit point.
- Lab O (Buffer overflow): This lab is done **individually** and is **graded automatically** by the submission system. By solving additional tasks, you can earn 1 merit point.
- Lab Z (Zip Bomb): This **optional** lab is done **individually** and is **graded automatically** by the submission system. By completing this lab, you can earn 1 merit point.

Exercises

The course has **several mandatory exercises** which are carried out either individually or in groups of any size. The goal of exercises is to provide hand-on experience of concepts from the lectures, by means of simple implementation tasks. The exercises are graded automatically (Pass/Fail) and a student should pass all assignments in order pass the course. The exercises will appear under [Exercises](https://canvas.kth.se/courses/64038/assignments) (<https://canvas.kth.se/courses/64038/assignments>) in due time.

Seminar (only for students in DD2395)

The course has **a mandatory seminar** which is carried out in **groups of 3 students**. The goal of seminar is expose students to computer security topics beyond the ones covered in the lectures, as well as to train their presentation and analytical skills. The seminar is graded as Pass/Fail and requires a presentation to the TAs at pre-scheduled seminar sessions. A student should pass the seminar in order pass the LAB part of the course. Details about the seminar will appear under [Seminar](https://canvas.kth.se/courses/64038/assignments) (<https://canvas.kth.se/courses/64038/assignments>) in due time. Students enrolled in DD2391 should do the seminar together with the Project (see below).

Project (only for students in DD2391 and DD2394)

Courses DD2391 Cybersecurity Overview and DD2394 Cybersecurity Project have **a mandatory project** which is carried out in groups of 4 students. The project is graded as Pass/Fail and requires a presentation at pre-scheduled project presentation sessions. A student should pass the project in order pass the course. Details about the project will appear under [Project](https://canvas.kth.se/courses/64038/assignments) (<https://canvas.kth.se/courses/64038/assignments>) in due time. The project is **the only activity** for students enrolled in DD2394, while students enrolled in DD2391 should in addition complete all the

required activities above. Students enrolled in DD2395 will not do the project. Students enrolled in DD2391 should do the project together with the Seminar (see above).

Examination and Grading

Courses DD2395 Computer Security and DD2391 Cybersecurity Overview are subject to a final written exam, which is graded on the scale A - F. Students that receive grade Fx will complement with an oral discussion to earn grade E. [Grade raising \(known as plussning\)](https://www.kth.se/en/student/studier/kurs/tentamen/plussning-1.1170812) (<https://www.kth.se/en/student/studier/kurs/tentamen/plussning-1.1170812>) is **NOT allowed** for these courses. The lab grade (Pass/Fail) is only reported if students have passed all mandatory (Pass/Fail) activities related to lab assignments, exercises and the seminar. Students aiming at final course grade A (B) should earn at least 2 (1) merit points in the lab assignments. Lab assignments allow to earn a total of 3 merit points, thus providing some flexibility. Below is the grade's protocol for each of the courses:

DD2395 Computer Security

- LAB (lab assignments, exercises, and seminar): Pass/Fail
- Written exam: A-F
- Final course grade:
 - Same as written exam, if the written exam grade is C or less. This is independent of merit points earned.
 - B, if the student has earned 1 merit point and written exam grade is A or B
 - A, if the student has earned 2 (or 3) merit points and written exam grade is A
 - The above assumes that the student has passed LAB.

DD2391 Cybersecurity Overview

- LAB (lab assignments, exercises, and project): Pass/Fail
- Project: Pass/Fail
- Written exam: A-F
- Final course grade:
 - Same as written exam, if the written exam grade is C or less. This is independent of merit points earned.
 - B, if the student has earned 1 merit point and written exam grade is A or B
 - A, if the student has earned 2 (or 3) merit points and written exam grade is A
 - The above assumes that the student has passed LAB and Project.

DD2394 Cybersecurity project

- Project: Pass/Fail
- Final course grade: Pass/Fail (same as the grade of project)

Acknowledgements

The course structure and many of the ideas, reading material, and slides are influenced or directly borrowed from other courses taught at Berkley, Cornell, MIT, Stanford, UCSD, and others.

Code of Honour

Students should be familiar with the [EECS School code of honor \(https://www.kth.se/en/eecs/utbildning/hederskodex\)](https://www.kth.se/en/eecs/utbildning/hederskodex) which we strictly follow. Cheating includes exchanging solutions between groups, not stating true contributions within a group, and not citing the sources.