Course Memo

In this course, DD2395 Computer Security (dasak), you will learn what measures there are to prevent, detect, respond to and recover from attacks on computer systems and how those attacks work. Along the way, you will pick up concepts, terminology, and a security mindset. In the **lab exercises (https://kth.instructure.com/courses/12372/pages/labs)** , you will apply cryptography to secure e-mail, build a firewall, exploit and fix vulnerabilities leading to buffer overflow and web attacks, in a **virtual machine (https://kth.instructure.com/courses/12372/pages/the-dasak-vm)** . You will get to pick a security topic to explore in a group and teach to others in a **seminar (https://kth.instructure.com/courses/12372/pages/seminars)** and in writing, learning from and critiquing those of other groups. You will also get **exercises (https://kth.instructure.com/courses/12372/pages/how-to-setup-and-submit-lab-o-and-exercises)** (writing small programs for a security problem) and short quizzes (related to some lectures) to do on your own, mainly for self assessment as you have unlimited attempts and the grading only reflects whether they have been successfully completed.

Schedule

See **http://www.kth.se/schema (http://www.kth.se/schema)** and **important dates, (https://kth.instructure.com/courses/12372/pages/important-dates) (https://kth.instructure.com/courses/12372/pages/important-dates)** as well as **lectures (https://kth.instructure.com/courses/12372/pages/lectures)** . Note that most lab sessions are optional help sessions (the assignments are mandatory but attending the help sessions is not), but there are some entries (e.g., presentation, seminar) where you will be asked to sign up for a specific time slot out of several choices.

Intended learning outcomes

The students should be able to:

- recognize threats to confidentiality, integrity, and availability of systems
- explain the basic computer security terminology and concepts and use them correctly
- find and apply documentation of security-related problems and tools
- analyze small pieces of code or system descriptions in terms of their security
- identify vulnerabilities of such code or descriptions and predict their corresponding threats
- select counter-measures to identified threats and argue their effectiveness
- compare counter-measures and evaluate their side-effects
- present and explain their reasoning to others

such that the students can:

- develop software or computer systems with security in mind
- go on to more specialized topics, such as network security

Course setup

6 ECTS, whereof 3 ECTS for lab exercises and seminar and 3 ECTS for an exam.

The course activities are lectures, lab exercises (both in groups and individual), exercises and quizzes (individual assignments, mandatory but not otherwise graded), and a seminar (in groups).

Examination and grading criteria

Lab assignments, exercises, quizzes, and the seminar are graded P/F; the exam part is graded A-F.

ILO	E/P	D	C	B
recognize threats to confidentiality, integrity, and availability of systems,	from simple examples		from simple system descriptions	
EXAMINATION	written exam, formative: quizzes, exercises			
explain the basic computer security terminology and concepts and use them correctly,	with few mistakes			
EXAMINATION	written exam and seminar report and presentation			
find and apply documentation of security-related problems and tools,	enough to solve labs and cover basics for seminar topic with some scientific resources			
EXAMINATION	labs, seminar report and presentation			
analyze small pieces of code or system descriptions in terms of their security,	with few mistakes		with demonstrated correct understanding	
EXAMINATION	labs and written exam			
identify vulnerabilities of such code or descriptions and predict their corresponding threats,	finding obvious problems with few mistakes		finding obvious problems correctly	
EXAMINATION	labs and written exam			
select counter-measures to identified threats and argue their effectiveness,	with some appropriate counter-measures and basic argumentation, with few mistakes		with some appropriate counter-measures and basic argumentation, correctly	
EXAMINATION	labs and written exam			
compare counter-measures and evaluate their side-effects,	from list with given effects, with few mistakes		with basic argumentation and list of side effects	
EXAMINATION	written exam			
present and explain their reasoning to others	with sufficient clarity for fellow students and for teachers to understand, with few mistakes		with enough relevant detail and few tangents	
EXAMINATION	lab solution presentations, seminar report and presentation , writter exam			

The written exam takes place in up to 2 parts.

1. multiple choice for grade E. 80% needed to pass (71% if you have all 3 possible bonus points). Note that simply guessing has an expected result of 50%.
2. open-ended questions solving security problems (analyzing systems or code, suggesting countermeasures), for grades D-A on the condition that E was achieved in the first part.

To prepare for the exam: Besides going to the lectures, taking notes, and studying the information given on each lecture page (slides, links, other material), do read the corresponding sections or chapters in the course books or otherwise research the topics further. This course covers a wide range of topics and it is not possible to go into enough depth for each topic just by the lectures alone. To check your knowledge, you can also look at old exams (**oldexams.zip (https://kth.instructure.com/courses/12372/files/2396034/download?wrap=1)** [zip file of pdfs]. Note that the format for these exams was different) and then read up some more on topics you've not mastered yet. As another check, go over the intended learning outcomes and evaluate your knowledge and skills.

Bonus points

You can collect bonus points, in total 3, in conjunction with some labs. Bonus points (BP) can be used for the exam. 1 BP = 3% of the written exam for E (max 9%), 3 BP = 1 C question or a partial A question. BP are only counted once in the course round; i.e., any BP used up to get an E are not available for higher grades and, conversely, any BP not needed to reach E can help get a higher grade. Unused bonus points do not expire, for example if you fail the regular written exam, you can use the BP at the re-exam.

Teachers

Sonja Buchegger **buc@kth.se (mailto:buc@kth.se)** (course responsible teacher, examiner)

Roberto Guanciale **robertog@kth.se (mailto:robertog@kth.se)** (teacher)

TBD (guest lecturers)

Anoud Alshnakat, Mohit Daga, Timoteus Ekenstedt, Matteo Gamba, Phillip Gajland, Md Sakib Nizam Khan, Andreas Lindner, Jan Van den Brand, Helena Rosenzweig, Mikhail Shcherbakov (teaching assistants)

Course literature

Free online -- **Ross Anderson, Security Engineering. (https://www.cl.cam.ac.uk/~rja14/book.html)** 3rd edition in progress, 2nd complete, both on the same page.

Dieter Gollmann, Computer Security free for KTH students via **library link (https://ebookcentral-proquest-com.focus.lib.kth.se/lib/kth/detail.action?docID=819182)** .

See reading recommendations for individual lectures for more detailed pointers to book chapters and sections.

Support/Funka

If you have a disability or other condition relevant to following courses, you can get support from Funka

Information in Swedish (https://www.kth.se/student/studentliv/funktionsnedsattning/ansok-om-stod-for-funktionsnedsattning-1.39736)

Information in English (https://www.kth.se/en/student/studentliv/funktionsnedsattning/ansok-om-stod-for-funktionsnedsattning-1.39736)

If you need accommodations or have suggestions on how to make the course more accessible, please contact the course leader.

Student representation

One or two students will represent the course participants, can be contacted to give feedback to the teachers, and will participate in discussions about the course evaluation.

Exchange students (incoming and outgoing)

If you are studying elsewhere and thus cannot attend the regular written and potential oral exam in January, you can get an oral examination (graded A-F) instead in December. There will be range of dates and times to choose from.

Contact and naming conventions

1. In relevant pinned discussion thread as a reply.
2. If nothing fits, post a new discussion or
3. Contact teacher or course responsible student(s)

- via Canvas or
- mail with subject [dasak19]

Name files dasak19<Purpose><Name|Group>.<ext>

Changes for this course round:

- updated and more detailed grading criteria
- visibility of Canvas set to public for KTH
- labs, Github and VM instructions, and assignments available from the start
- canvas navigation: less clicking, more scrolling
- ongoing effort: more automated continuous grade reporting on Canvas
- return to strict time slot adherence for booked solution presentations
- updated VM