Aalto University

Starting at 14:15

Welcome to the Information Security course!

Tuomas Aura
CS-C3130 Information security

Aalto University 2023

About the teachers

- Lecturer: Tuomas Aura
  - Professor at Aalto since 2008
  - Microsoft Research, UK, 2001–2009; teaching at UCL
  - Doctoral degree at TKK in 2000, MSc (Tech) in CS in 1996
  - Research: security of Internet protocols; designing secure protocols and systems; security analysis of new technologies
- Co-teacher: Lachlan Gunn
  - University lecturer, Academy of Finland postdoctoral researcher
  - Research: platform security (OS, compiler, CPU)

Course contacts

- Course materials and up-to-date info in MyCourses: https://mycourses.aalto.fi/course/view.php?id=41069
- MyCourses front page and announcements for the latest info
- MyCourses discussion forum for public questions

- Email: cs-c3130@aalto.fi for personal questions

  Please use this address for all course-related email.
  Avoid sending email directly to the teachers.

- Full course staff: Tuomas Aura, Lachlan Gunn, Jacopo Bufalino, Jose Luis Martin Navarro, exercise assistants

Learning objectives

- Learn concepts and abstractions for thinking and talking about information security
- Learn the adversarial mindset of security engineering. Be able to model threats and analyze the security of a system critically, from the attacker’s viewpoint
- Understand the purpose and function of several security technologies, as well as their limitations
  - security policies , authentication, access control, cryptography, network protocols, identity management etc.
- Have hands-on experience of security flaws in software, to be a better programmer
- Basis for further study and research

Prerequisite knowledge

- Writing and reading program code in many languages
- Broad knowledge of information technology
  - Linux shell, Windows, databases, web programming, internet, C

FAQ: Can I take this course?

- Yes, if you really want to. Nothing is very difficult, but the less you know, the more extra work there will be to learn the technologies.
- The more you know about IT, the more you can focus on security.
- Advice: Budget some hours for each exercise round and stop when they have been used. Do not feel bad about parts B and C.

Lectures and flipped classroom

- Recorded lectures published during lecture period I
  - Streaming and download from Panopto, link in MyCourses
  - Approximately 10 lectures of 1-2 hours each, split to smaller parts
  - Pro hint: if the lecture is too slow, play at 150% speed
- Lecture slides will be in MyCourses
  - Handouts include some helpful pages not shown in the lectures
  - Pages that can be safely skipped are marked with Extra material
- Flipped classroom sessions to support learning of selected lecture content
  - Tue and Thu at 14:15-16 on campus (variable location!) starting from the second week

Weekly exercises

- Exercises provide hands-on experience especially in software security to make us better programmers
- Exercises are not mandatory but strongly recommended
- 5 weekly rounds of exercises. Deadline Fridays at 18:00. First deadline on 15 September 2023
- Problems published in MyCourses at least one week earlier
- No mandatory exercise sessions to attend
- Course assistant reception hours for help and advice:
  - Tue, Wed and Thu at 16:15-18 on campus

Extensive log files from the exercise platform will be used for course development and research. Please do not include personal information such as your name in the inputs.

Advice for the exercises

- Programming skills are required for the exercises
- Try to solve all problems at least partly
- Exercises have two or three parts:
  - Part A should be easy (10 points)
  - Part B should be more difficult (10 points)
  - Parts C is for bonus points and challenge (10 points)
- Do not expect to solve all parts! Try to do at least part A
  - Join the exercise sessions for help, especially on part A
- Individual work: Discuss with other students but do all practical experiments independently

Exam and course grading

- The exam will be on campus during the exam week
- Grading based on a weighted sum of exam and exercise points:

  total_points = exam + round_up(exercises / 10)

- Maximum points: 30+10 (exam + 5 * exercise parts A and B)
  - With bonus points for exercise parts C, possible to exceed this
- Collect at least 40% of the total points (≥16) to pass the course

The exam registration is separate and not including in the course registration. Please register for the exams in Sisu. In this course, even the first exam (in October) is not automatically included.

Course plan

Lectures on information security:

Course intro

1. Access control models
2. Access control in operating systems
3. User authentication
4. Software security
5. Cryptography
6. Data encryption
7. Security protocols
8. PKI and web security
9. Threat analysis
10. Identity management

Note: The exercises focus on software security while the lectures and flipped classroom cover information security broadly

Some changes possible

Exercises :

1. Access control in Linux and Windows
2. Software and web security 1 (SQL injection)
3. Software and web security 2 (web security)
4. Software and IoT security 3 (buffer overrun)
5. Software and web security 4 (XSS)

Recommended reading

- Best coverage of the course syllabus :
  - William Stallings, Computer Security: Principles and Practice, 5th ed. 2023 / 4th ed. 2018
- Better books by real experts, but less content covered:
  - Matt Bishop, Computer Security. Art and Science, 2018 (for prospective research students)
  - Ross Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd ed., 2020 (good reading)
- Read lecture slides and search for online sources on each lecture topic!

FAQ

- What does the exam cover?
  - Mainly lectures and flipped classroom discussion but also the exercises and general knowledge of the course area
- Why are there three exams?
  - You can choose a time that fits your schedule – or take the exam up to three times. The grade will be based on the best result. However, if you take the first exam, you don’t need to re-watch the lecture later
- What is the difference between normal points and bonus points?
  - None. The exam points are all added together. Also, the points are not capped
- Can you publish the grade boundaries?
  - Sorry, no. The grading will be adjusted depending on how difficult the exam is this time
- Can we have Slack/Facebook/Discord/Telegram/Instagram for exercise support and sharing hints?
  - Sorry, no. The best we can do is the exercise support sessions and email alias. Please do not share your solutions online; it will spoil the fun for others
- Can I see some old exam questions?
  - Yes, they are at https://tenttiarkisto.fi/courses/?q=cs-c3130