Aalto University

Welcome to the introductory information security course!

Tuomas Aura
CS-C3130 Information security

Aalto University, 2021 course

About the lecturer

- 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 computer science in 1996
- Research themes:
  - Security protocol engineering, e.g., mobility, device bootstrapping
  - Security analysis of new technologies

Course contacts

- Course materials and up-to-date info in MyCourses: https://mycourses.aalto.fi/course/view.php?id=32363

- MyCourses discussion forum for public questions

- Email: cs-c3130@aalto.fi

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

- Course staff: Tuomas Aura, Lachlan Gunn, Aleksi Peltonen, Jacopo Bufalino, exercise assistants

Course goals

- Learn concepts and abstractions of 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, privacy tools etc.
- Have hands-on experience of security flaws in software, to be a better programmer
- Basis for further study and research

Prerequisite knowledge

- Ability to program 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.
- Budget some hours for each exercise round and stop when they have been used. Do not feel bad about not completing parts B and C.

Lectures

- Recorded lectures published two per week in lecture period I
  - Streaming and download from Panopto, link in MyCourses
  - Approximately 11 lectures of 1-2 hours each, cut to smaller parts
- Lecture slides will be in MyCourses
  - Handouts include some 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 – new experiment this year

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 Friday 18:00.
  First deadline on 24 September 2021
- 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 in Zoom; sessions on campus depending on demand

Extensive log files from the exercise platform will be used for course development and research.

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
  - If exam halls cannot be used, it will be in the EXAM studio

- 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)
  - plus a few bonus points for exercise parts C

- Collect at least 40% of the total points (≥16) to pass the course

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
11. Privacy

Summary

Note: The exercises focus on software security while the lectures(+exam) cover information security broadly

Subject to change

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, 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 (Highly recommended reading. Used also in CS-E4350 Security Engineering in spring 2021.)

- Search for online sources on each lecture topic!