Aalto University

Platform Security: Introduction

Theme of this course

Information security: a broad overview

Security engineering: what can you do to help?

Platform security: what can your platform do to help?

Goal of the course

Make you into a more active consumer of platform security features

Learn what help to expect from your...

- OS
- Compiler
- CPU

Course structure

Lectures

Exercises

- Weekly exercises
- Short presentations

Lectures

What your OS offers

- Sandboxing
- Access control

What your compiler offers

- Run-time security

What your hardware offers

- Secure boot
- Trusted Platform Module
- Trusted execution environments

Weekly exercises

Exercises contain both written and practical components

Exercise topics & release dates:

- 10.1 **Sandboxed environments**
- 17.1 **Access control**
- 21.1 **Memory safety vulnerabilities**
- 28.1 **Memory safety defences**
- 4.2 **Hardware security mechanisms**

Students will present their results to the class during Thursday sessions

- Participation is necessary to complete the course

Weekly rhythm

Tuesday

- New lecture
- New exercise released

Monday

- Exercise due (evening)

Wednesday

- Exercise feedback made available
  - Not a promise, as registrations have exploded since we published the schedule

Thursday

- Present your work in exercise session

Course grade

To pass the course:

- Submit an exercise each week
- Attend at least four out of five exercise sessions (starting 19.1)
  - Active participation needed: be prepared to present your answers.

To get top marks:

- As above, but provide correct answers in exercise

Scores needed for grades 1–5 to be determined later