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 tools

→ Learn what help to expect from your…
- OS
- Compiler
- CPU
- ⋮

Course structure

Lectures

- Videos on MyCourses
- Discussion sessions

Project

- Weekly exercises
- Short presentations

Exam

Lectures

What your OS offers

- Access control
- Sandboxing
- Mobile platforms

What your compiler offers

- Run-time security

What your CPU offers

- Trusted execution environments

Weekly exercises

Build a basic container system

29.4 ├ Write a program to containerize
 6.5 ├ Lock the program to a new root filesystem
13.5 ├ Add runtime permissioning support
20.5 ├ Secure against (some) runtime attacks
27.5 └ Add a hardware-supported keystore

Discussion sessions

Tuesdays

- Discuss the current lecture
- Start working on the new exercise

Thursdays

- Discuss your solutions in groups
- Make a presentation to the class

Active participation required

- Submit your attempt on MyCourses by the end of Wednesday
- Discuss during sessions on Thursday

Course grade

50% Exercise participation

For full marks:

- Submit an exercise attempt each week
- Attend at least four exercise sessions (starting 29.4)

50% Exam