Secure Software and Hardware Security

Mihai Ordean
Marius Muench

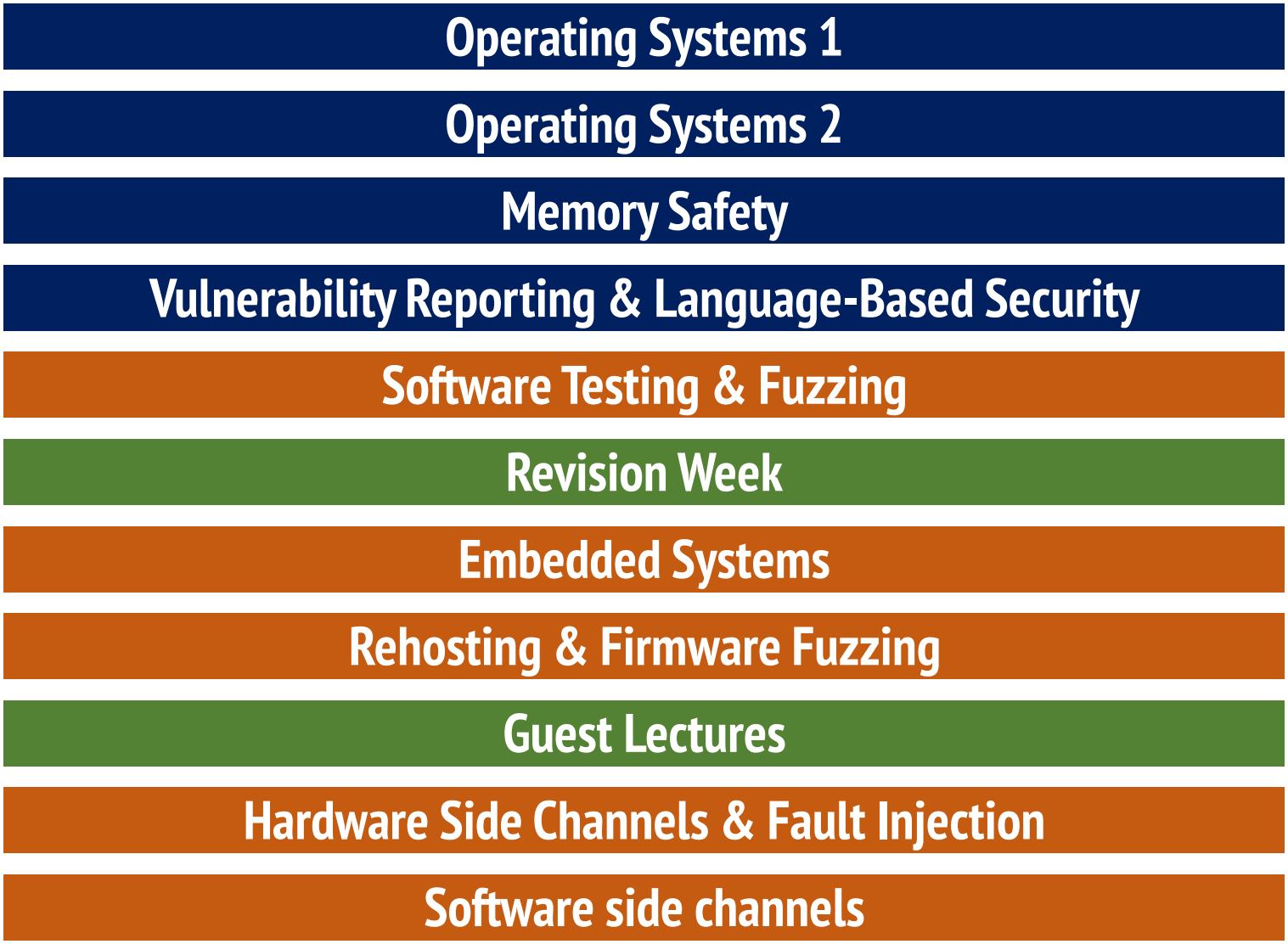
Mihai Ordean

Marius Muench

Teaching support

- Matthew Bowden
- Jinjin Wang
- Yusuf Hagezy

This module


Operating Systems 1
Operating Systems 2
Memory Safety
Vulnerability Reporting & Language-Based Security
Software Testing & Fuzzing
Revision Week
Embedded Systems
Rehosting & Firmware Fuzzing
Guest Lectures
Hardware Side Channels & Fault Injection
Software side channels
Mihai Ordean
Marius Muench

Lectures

- Two slots per week: Thursday and Friday

  - **Thursday 5pm-6pm** in Y3 - Y3-G33
    - **Normal Lecture**
  - **Friday 1pm-2pm** in Sport and Exercise Sciences - SPTX-LT2 (G85)
    - **Normal Lecture**

  - **Thursday 6pm-7pm** in Y3 - Y3-G33
    - **Extra content/Practical session** (to be announced on a week-by-week basis)

Assessed Exercises

- There are two **group assessments**, each worth 10% of your mark (20% total)
    - Week 5-7: Assessment 1 (2 weeks total time)
    - Week 8-10: Assessment 2 (2 weeks total time)

Unassessed Exercises and Questions

- You MUST make sure you understand the questions
  - If you don't you should see me, or Marius, during our office hours.

- You SHOULD be able to answer most of the informal questions in from your lectures
- You can bring your work to us during our office hours for discussion and feedback.

Lectures overview

1st part

Areas covered:

- Operating systems and virtualisation ”security”
- Memory safety
- Language-based security and common vulnerabilities and exposures (CVEs)

Lectures overview

- Operating systems
  - OS components,
    - Memory layout, MMU
    - Processes
    - Threads
    - System calls, etc.
  - Sandboxing as a security feature
  - Virtualisation and emulation

Lectures overview

- Memory safety
  - common classes of memory safety issues
  - countermeasures.

Lectures overview

- Programming language –based security
  - Safety related compiler features
  - Safe and unsafe languages
- Reporting vulnerabilities and CVEs