

# AN TOÀN HỆ ĐIỀU HÀNH (OPERATING SYSTEM SECURITY)

## Đề cương chi tiết (Course Syllabus)

### 1. General Information

**Course name:** An toàn hệ điều hành (Operating System Security)  
**Course code:** SEC1419\_CLC  
**Course type:** Selective  
**Number of credits:** 2

### 2. Objectives

#### *Knowledge:*

The aim of this course is to provide students with basic knowledge of operating system security.

#### *Skills:*

On successful completion of this course a student will be able to apply and evaluate security measures for operating systems and their services.

#### *Attitude:*

Students are required to attend the classes and complete assignments/projects.

### 3. Abstracts

This course provides students with basic knowledge of operating system security, including hardware-based security mechanisms; security for basic services of operating systems; security models and security assessment for operating systems.

### 4. Teaching and learning methods

Lectures: 16h  
Exercises: 4h  
Projects: 6h  
Labs: 4h  
Individual reading: 0h

**5. Prerequisites:** Computer Architecture and Operating Systems - INT1325\_CLC

### 6. Learning outcomes

After completing this course, the student is able to:

[CLO1]: Explain the basic concepts and knowledge of operating system security;

[CLO2]: Apply and evaluate security measures for operating systems and their services.

### 7. Assignment criteria

Learning outcomes	Assignment criteria
[CLO1]: Explain the basic concepts and knowledge of operating system security	Chapter 1, Chapter 2, Chapter 3, Chapter 4, Chapter 5
[CLO2]: Apply and evaluate security measures for operating systems and their services	Chapter 3, Chapter 4, Chapter 5

## 8. Outlines

### Chapter 1 Introduction to operating system security

- 1.1 Overview of operating system security
- 1.2 Security architecture issues
- 1.3 Security policies
- 1.4 Security kernel

### Chapter 2 Hardware-based security mechanisms

- 2.1 Process protection
- 2.2 Memory protection
- 2.3 I/O control
- 2.4 Virtualization

### Chapter 3 Security for basic services of operating systems

- 3.1 Process management
- 3.2 Memory management
- 3.3 Trusted computing platforms
- 3.4 File systems
- 3.5 Security analysis of basic services for Windows and Linux operating systems

### Chapter 4 Security Models

- 4.1 The roles and characteristics of security models
- 4.2 State machine models
- 4.3 Harrison-Ruzzo-Ullman models
- 4.4 Other models

### Chapter 5 Security Assessment

- 5.1 Overview of security specifications
- 5.2 Security specification verification techniques
- 5.3 Data and algorithm decomposition methods
- 5.4 Program code verification techniques

## 9. Required Textbooks

- [1] Andrew S. Tanenbaum, Herbert Bos, *Modern Operating Systems*, 4th Edition, Pearson Education Inc., 2015.

## 10. Suggested Textbooks

- [2] Phạm Hoàng Duy, *Bài giảng An toàn hệ điều hành*, Học viện Công nghệ Bưu chính Viễn thông, 2017.

- [3] Abraham Silberschatz, Peter B. Galvin, Greg Gagne, *Operating System Concepts Essentials*, John Wiley & Sons Inc., 2014.
- [4] Mehedi Al Mamun, *Operating Systems Security: Linux*, LAP Lambert Acad. Publishing, 2011.
- [5] Seymour Bosworth. M.E. Kabay, Eric Whyne, *Computer Security Handbook*, 6th Edition, John Wiley & Sons, 2014.

## 11. Schedule

Main contents	Duration	Specific contents
Chapter 1 Introduction to operating system security	3h lecture 1h project	1.1 Overview of operating system security 1.2 Security architecture issues 1.3 Security policies 1.4 Security kernel
Chapter 2 Hardware-based security mechanisms	2h lecture 1h exercise 2h project 1h lab	2.1 Process protection 2.2 Memory protection 2.3 I/O control 2.4 Virtualization
Chapter 3 Security for basic services of operating systems	5h lecture 1h exercise 2h project 1h lab	3.1 Process management 3.2 Memory management 3.3 Trusted computing platforms 3.4 File systems 3.5 Security analysis of basic services for Windows and Linux operating systems
Chapter 4 Security Models	3h lecture 1h exercise 2h project 1h lab	4.1 The roles and characteristics of security models 4.2 State machine models 4.3 Harrison-Ruzzo-Ullman models 4.4 Other models
Chapter 5 Security Assessment	3h lecture 1h exercise 1h project 1h lab	5.1 Overview of security specifications 5.2 Security specification verification techniques 5.3 Data and algorithm decomposition methods 5.4 Program code verification techniques

## 12. Grading Policy

Attendance:	10%
Mid-term exam/exercises:	10%
Course projects:	30%
Final examination:	50%