

CCY4304 Operating Systems Security**COURSE INFORMATION**

Prerequisites	Academic Year & Level		Teaching Methods			Credit Hrs.
	Year	Semester	Lecture	Tutorial	Laboratory	
CCY2001 and CCS3203	4	7/8	2	--	2	3

COURSE AIM

To get the students to:

- Identify security issues in operating systems
- Understand and experiment with access control models
- Apply buffer overflow defences
- Understand and experiment with OS kernel security mechanisms
- Understand virtualization security alternatives
- Understand and experiment with mobile OS security

COURSE WEEKLY CONTENTS

- 1 Course Introduction and Syllabus discussion
- 2 Security Issues in Operating Systems
- 3 Buffer Overflow Attacks and Defences
- 4 Access Control Fundamentals
- 5 Access Control: Verifiable Security Goals
- 6 OS Access Control Case studies
- 7 7th week Assessment
- 8 OS Kernel Security Mechanisms
- 9 OS Kernel Security Mechanisms (cont.)
- 10 Virtualization Security
- 11 Virtualization Security (cont.)
- 12 12th week Assessment
- 13 Mobile OS Security
- 14 Mobile OS Security (cont.)
- 15 Operating Systems Security Case Studies and Projects Presentations

STUDENT GRADING & ASSESSMENT

Weeks	Exams	Assign.	Quizzes	Reports	Present.	Lab.	Total
1 to 7			30				30
8 to 12			20				20
13 to 15			10				10
16 or 17			Final Exam				40

REFERENCES

- Textbook** Trent Jaeger, Operating System Security (Synthesis Lectures on Information Security, Privacy, and Trust), Springer
 William Stallings, Operating Systems: Internals and Design Principles, Pearson.