

UNDERGRADUATE PROGRAM IN COMPUTER SCIENCE
DEPARTMENT OF COMPUTER ENGINEERING
FACULTY OF INTELLIGENT ELECTRICAL AND INFORMATICS TECHNOLOGY

Module name	Computer System Security	
Module level	Undergraduate	
Code	EC184704	
Courses (if applicable)	Computer System Security	
Semester	7 / Fall (Gasal)	
Contact person	Dr. Surya Sumpeno, S.T, M.Eng.	
Lecturer	Dr. Surya Sumpeno, S.T, M.Eng.	
Language	Indonesia / English	
Relation to curriculum	Undergraduate degree program, mandatory, 7 th semester.	
Type of teaching, contact hours	Lecture, < 60 students, 170 Minute 3 SKS	
Workload	1. Lectures: 3 x 50 = 150 minutes (2.5 hours) per week. 2. Exercises and Assignments: 3 x 60 = 180 minutes (3 hours) per week. 3. Private study: 3 x 60 = 180 minutes (3 hours) per week.	
Credit points	3 credit points (sks).	
Requirements according to the examination regulations	A student must have attended at least 75% of the lectures to sit in the exams.	
Mandatory prerequisites	Numerical Methods, Internet Networking Engineering, Distributed Systems	
Learning outcomes and their corresponding PLOs	CLO-1 Students are able to explain and understand the basics of security its policies, basic security principles, and cryptography basics. CLO-2 Students are able to explain and apply the concept of access control and system file security. CLO-3 Students are able to explain and apply the concept of security to software, input handling from programs, race conditions, and memory exploitations. CLO-4 Students are able to explain and understand malicious software, viruses, worms, rootkits, and botnets. CLO-5 Students are able to explain and implement the concepts of network threat, network security, and intrusion detection.	PLO-3 PLO-3 PLO-4 PLO-3 PLO-3 PLO-4 PLO-5

	<p>CLO-6 Students are able to explain and apply the concept of SSL, secure email, and PKI.</p> <p>CLO-7 Students are able to explain and apply the concept of web security and its prevention methods.</p>	<p>PLO-5 PLO-6</p> <p>PLO-5 PLO-6</p>
Content	<p>In this course, students will learn about computer system security and its problems. Students will be exposed to basic security concepts on networks, software, infrastructure, and viruses. Topics include reviewing computer networking materials and operating systems, software security, passwords, authentication, privacy, data integrity, anonymity, security on network services, infrastructure security, firewalls, viruses, intrusion detection and network attacks.</p>	
Study and examination requirements and forms of examination	<ul style="list-style-type: none"> • In-class exercises • Quiz 1 and 2 • Assignment 1, 2, 3 • Mid-term examination • Final examination 	
Media employed	<p>LCD, whiteboard, websites (myITS Classroom).</p>	
Assessments and Evaluation	<p>CO-1: Question no 1 in midterm exam (10%) CO-2: Question no 2 in midterm exam (10%) CO-3: Question no 3 in midterm exam (10%), quiz 1 (5%) CO-4: Assignment 1 (5%), question no 4 in midterm exam (10%), Quiz 2 (5%) CO-5: Question no 1 in final exam (10%), question no 2 in final exam (10%) CO-6: Assignment 2 (5%), question no 3 in final exam (10%) CO-7: Assignment 3 (5%), question no 4 in final exam (5%)</p>	
Reading List	<ol style="list-style-type: none"> 1. William Stallings dan Lawrie Brown, "Computer Security: Principles and Practice, 2/E", Prentice Hall, 2012 2. Georg Hager dan Gerhard Wellein, "Introduction to High Performance Computing for Scientists and Engineers (Chapman & Hall/CRC Computational Science)", CRC Press, 2010. 	